Supuestos de transmisión de datos fuera de la organización

PID_00248555

Belén Duran Cardo

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Índice

Introducción

Sin duda estamos ante un momento clave de la regulación del derecho a la protección de datos. La Directiva 95/46/CE, de 24 de octubre, 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 (Directiva 95/46/CE), claramente había quedado obsoleta ante el desarrollo tecnológico y se había mostrado incapaz de armonizar suficientemente las normativas nacionales.

La aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), que desplaza la normativa nacional de los Estados miembros a partir del día de su aplicación, el 25 de mayo de 2018, ha intentado solucionar los problemas que la Directiva 95/46/CE no pudo resolver y supone un punto de inflexión en esta materia.

Ante este período de transición nos acercaremos en este módulo a la regulación de los supuestos de transmisión de los datos personales. Mientras que en la Directiva 95/46/CE todos los tratamientos tenían la misma regulación y así se ha mantenido en el RGPD, en la legislación española hemos contado con una regulación específica para la cesión de datos. Nuestra legislación también ha desarrollado ampliamente la figura del encargado del tratamiento, que tenía su base regulatoria en el artículo 12 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

Con el fin de poder aproximarnos al RGPD, pero sin olvidar estos antecedentes de nuestra propia legislación, nos referiremos, en primer lugar, a la regulación de la cesión de datos que teníamos en nuestra normativa y que ha dado paso a la inexistencia de esta regulación específica en el RGPD.

En segundo lugar, recorreremos las previsiones que el RGPD recoge sobre la figura del encargado del tratamiento, que se ha convertido en un actor relevante en esta materia. De este modo, abordaremos su definición y la distinción entre encargado y responsable, así como la relación contractual entre ambos y, finalmente, las obligaciones que tiene el encargado.

A continuación, con el fin de tener una visión más práctica, plantearemos las principales problemáticas que nos encontramos en los servicios de *cloud computing*. Hemos elegido estos servicios ya que constituyen uno de los instrumentos que contribuyen a la evolución tecnológica y a la creación de nuevos modelos de negocio.

Finalmente, nos referiremos a los mecanismos de autorregulación que introduce el RGPD, como colofón al nuevo enfoque de responsabilidad proactiva adoptado en el texto.

1. La cesión de datos: de una regulación específica en la LOPD a la carencia de la misma en el RGPD

La cesión de datos es un tratamiento de datos, tal como se deriva de la definición de tratamiento.

Tratamiento de datos

Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias (art. 5.1.t RLOPD).

A diferencia de la Directiva 95/46/CE, que no realizaba ninguna distinción entre la cesión y los otros tratamientos de datos, en la legislación española se estableció una regulación específica para este tratamiento en concreto. Esta regulación está llamada a desaparecer con la aplicación del Reglamento general de protección de datos, que, al igual que la Directiva 95/46/CE, no ha hecho distinción entre tratamientos y ha establecido una regulación común a todos ellos.

1.1. El concepto de cesión

El concepto de cesión o comunicación de datos se encuentra en la LOPD: «Toda revelación de datos realizada a una persona distinta del interesado» (art. 3.i) LOPD).

En el 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 (RLOPD), se añade que la cesión es un tratamiento de datos (art. 5.1.c RLOPD), tal como hemos indicado.

Esta definición se centra en el acto de revelación de los datos, de forma que no solo se incluirá el acto mediante el que un sujeto transmite datos a otro, sino también el acto que implica que un sujeto ponga a disposición de otro u otros los datos, sin tener claro si este sujeto o sujetos receptores llegarán a captar los datos.

Por ejemplo, si publicamos datos personales en internet, ello implica una revelación pero no tiene necesariamente que implicar que un tercero capte esos datos para hacer un uso de ellos (Messía, 2003, págs. 58-59).

El Tribunal Supremo, en STS de 17 de septiembre de 2010, FJ 5, sostiene que el artículo 3.i) LOPD «no contempla, en la definición que ofrece de cesión o comunicación de datos, la necesidad o requisito de que la revelación vaya acompañada de una entrega material de los datos ni, por supuesto, de una incorporación al fichero del cesionario. Lo único que exige el precepto legal es la acción de revelar, esto es, la de hacer saber cosas que se mantenían ocultas, sin requerir que tal forma de proceder revista una forma determinada».

Referencia bibliográfica

J. Messía de la Cerda (2003). *La cesión o comunicación de datos de carácter personal*. Cizur Menor: Aranzadi.

Las cesiones de datos que se consideran tratamiento son aquellas resultantes de comunicaciones, consultas, interconexiones y transferencias (art. 3.c LOPD y 5.1.t RLOPD), por lo que se puede observar la naturaleza técnica del término cesión que pretende incorporar cualquier transmisión de datos.

El sujeto que cede los datos o cedente se configurará como responsable, ya que decidirá sobre este tratamiento (Messía, 2003, págs. 61-62).

El sujeto receptor de los datos es el destinatario o cesionario que se define como:

> «la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados» (art. 5.1.h) RLOPD).

Debe entenderse que la responsabilidad del sujeto cesionario dependerá de la conducta que este lleve a cabo (Durán, 2016, pág. 461).

Referencia bibliográfica

B. Durán (2016). *La figura del responsable en el derecho a la protección de datos*. Madrid: Wolters Kluwer.

La regulación general de la cesión se halla principalmente en el artículo 11 LOPD y en los artículos 10 y 12.2 RLOPD. Pero, además, debemos tener en cuenta las regulaciones específicas dependiendo de si estamos ante ficheros de titularidad pública o privada, y también para el caso de tratar datos especialmente protegidos.

Debe tenerse en cuenta que, cuando se publica información en una página web, hay una cesión de datos –como puede constatarse leyendo el Informe 261/2010 sobre actas de ayuntamientos– porque el punto es que quien publica ya es cedente por el hecho de publicar la información. Quien consulte dicha información será cesionario; sin embargo, si no hace nada más no habrá oportunidad de aplicarle la normativa.

1.2. Requisitos para ceder datos en la regulación general

Para poder comunicar datos se establecen dos requisitos en la regulación general: a) el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario, y b) el previo consentimiento del interesado (art. 11.1 LOPD).

El primer requisito establece el carácter instrumental de la cesión que impediría la realización de una cesión cuyo único objetivo fuera la cesión en sí misma. La cesión debe conectarse con la relación entre ambas partes, cedente y cesionario, y con sus actividades legítimas. Asimismo, esto implica que la cesión responda a unas funciones de cedente y cesionario que deben ser legales.

Al igual que para poder realizar cualquier tratamiento de datos, el consentimiento también se configura en este caso como la pieza clave que asegurará que sea el titular de los datos quien asuma el control sobre los mismos[1]. El consentimiento del interesado se encuentra definido en la LOPD como «toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen». A estos requisitos del consentimiento se añade, en el artículo 11 LOPD, para la cesión, la característica de que debe ser previo. No obstante, el RLOPD añade también esta palabra para definir los requisitos del consentimiento para poder tratar datos, no solo para la cesión (art. 10.1 RLOPD).

(1)STC 292/2000, de 30 de noviembre de 2000, FJ 7.

En el caso del consentimiento para realizar cesiones, se establece la nulidad del mismo si la información que se facilite al interesado no le permitiera conocer la finalidad a que destinarán los datos, cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretendan comunicar (arts. 11.3 LOPD y 12.2 RLOPD)[2]. Por lo tanto, el legislador no ha considerado imprescindible que el titular conozca la identidad del cesionario para poder otorgar un consentimiento válido. No obstante, el hecho de no individualizar a los cesionarios no parece acorde con la obligación general de informar sobre los destinatarios (art. 5.1.a) LOPD).

(2)Por tanto, no se exigiría la determinación de quien es el cesionario, excepto, como veremos, en los ficheros de titularidad privada. La STC 292/2000, de 30 noviembre, FJ 13, en este sentido indicaba que «el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y circunstancias como del destino de estos, pues solo así será eficaz su derecho a consentir [...] Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta».

Este consentimiento para la cesión, del mismo modo que sucede con el que se otorga para tratar datos, es revocable (art. 11.4 LOPD)[3].

(3)Aunque no se especifica, como sí sucede con el consentimiento general para tratar datos, que la revocación no tiene efectos retroactivos, debe entenderse que también se aplicará a este caso de la cesión. También entendemos que sería aplicable la regulación que el artículo 17 RLOPD establece para llevar a cabo esta revocación del consentimiento.

Las excepciones al requisito del consentimiento (que no al relativo al cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario) son, según su redacción en la LOPD:

«a) Cuando la cesión está autorizada en una ley; b) cuando se trate de datos recogidos de fuentes accesibles al público; c) 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 solo será legítima en cuanto se limite a la finalidad que la justifique; d) cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los jueces o tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas; e) cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos; f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica» (art. 11.2 LOPD).

Vemos que la mayoría de supuestos estarían en línea con los establecidos para el tratamiento general de datos (art. 6 LOPD).

La ley habilitaría el tratamiento general y el específico de la cesión. El RLOPD especifica que debe tratarse de una norma con rango de ley o una norma de derecho comunitario (10.2.a RLOPD), y que pueden darse dos supuestos: cuando la cesión tenga por objeto la satisfacción de un interés legítimo del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 LOPD, o cuando la cesión sea necesaria para que el responsable del tratamiento cumpla con un deber que le imponga una de dichas normas.

De esta forma, no es necesario que aparezca estipulada de forma expresa esta cesión en las normas. Basta con que la cesión se precise para que el responsable cumpla un deber que sí esté previsto expresamente en las leyes, o que sea para la satisfacción de un interés legítimo, si no prevalece el interés o los derechos y libertades de los interesados.

En lo que respecta a la posibilidad de ceder datos sin consentimiento del afectado, cuando se trate de datos recogidos de fuentes accesibles al público, esta posibilidad debe quedar sustituida por la aplicación directa del artículo 7.f) Directiva 95/46/CE, en virtud de la sentencia del Tribunal de Justicia de la UE de 24 de noviembre de 2011, ASNEF, FECEMD/Administración del Estado, C-468/10 y C-469/10[4].

(4)En esta sentencia el TJUE estableció la incorrecta transposición de este artículo a la legislación española, en concreto, al artículo 10.2.b) RLOPD, que fue anulado, en consecuencia, por el Tribunal Supremo en STS de 8 de febrero de 2012. El artículo 7.f) Directiva 95/46/CE establece una habilitación para tratar datos si es para satisfacer el interés legítimo del responsable a quien se comuniquen los datos, siempre que este interés prevalezca sobre el interés o los derechos y libertades fundamentales del interesado. En cambio, el artículo 10.2.b) RLOPD, al igual que hacía el artículo 6.2 *in fine* LOPD, añadía a estos dos requisitos enunciados en el artículo 7.f) el de que los datos debían figurar en fuentes accesibles al público. El TJUE consideró que, por lo tanto, se estaba limitando la aplicación del supuesto. Asimismo, el TJUE afirmó que el artículo 7.f) Directiva 95/46/CE tenía efecto directo, lo que implica que esta disposición pueda ser invocada por cualquier particular y aplicada tal cual por los órganos jurisdiccionales. Pese a que el Tribunal Supremo no anuló ninguno de los artículos 6.2 *in fine* y 11.2.b LOPD, estos deben quedar sustituidos por la aplicación directa de este artículo 7.f) Directiva 95/46/CE (Durán, 2016, págs. 464-465). El hecho de que los datos figuren en fuentes accesibles al público debe tomarse como un elemento más de ponderación que puede hacer más fácil que se prime el interés del responsable sobre el de los interesados, tal como han indicado el mismo TJUE, la AEPD en su Informe 111/2012 y la Audiencia Nacional en sentencia de 31 de mayo de 2012, FJ 3.

La relación jurídica aceptada por el titular de los datos se equipararía con la relación negocial, laboral o administrativa que justificaría el tratamiento general de los datos.

La urgencia que permitiría ceder datos de salud es similar al interés vital que habilitaría al tratamiento de datos.

No halla, sin embargo, su paralelismo en la regulación del artículo 6 LOPD, la comunicación que podrá realizarse al Defensor del Pueblo, el Ministerio Fiscal o los jueces o tribunales o el Tribunal de Cuentas o las instituciones autonómicas con funciones análogas. En el RLOPD se añade que esta cesión deberá realizarse en el ámbito de las funciones que la ley atribuya expresamente a estos sujetos. Tampoco se encuentra reflejo en el artículo 6 LOPD de la posibilidad de ceder datos entre Administraciones públicas cuando el tratamiento posterior de los datos tuviera fines históricos, estadísticos o científicos. A este respecto hay que indicar que la LOPD incluye una regulación específica sobre la comunicación de datos en ficheros de titularidad pública, así como también respecto a ficheros de titularidad privada, como a continuación abordaremos.

1.3. Regulaciones especiales de la cesión de datos

La LOPD incluye disposiciones sectoriales en su título IV para los ficheros de titularidad pública y privada.

En el caso de los ficheros de titularidad pública, cuya regulación se analizará en detalle en otra asignatura, baste indicar que se permite la cesión sin consentimiento en este ámbito en los siguientes casos: cuando sea con fines históricos, estadísticos o científicos, cuando una Administración pública obtenga o elabore los datos con destino a otra y cuando sea para el ejercicio de competencias idénticas o que versen sobre las mismas materias (arts. 21 LOPD y 10.4.c) RLOPD).

Respecto a los ficheros de titularidad privada, el artículo 27 LOPD establece una obligación específica de información en el momento en que el responsable del fichero efectúe la primera cesión de datos. En concreto, el responsable debe informar de la finalidad del fichero, la naturaleza de los datos que hayan sido cedidos y el nombre y dirección del cesionario. Esta obligación no existirá cuando la cesión venga impuesta por ley y en los supuestos establecidos en los apartados 2, letras c), d), e) y 6 del artículo 11. Estos apartados son prácticamente aquellos supuestos en los que no se precisa solicitar el consentimiento para ceder datos.

Este precepto es bastante confuso por diversas razones. Así, por un lado, al mencionarse como parte del contenido de la información los datos «que hayan sido cedidos», parece como si esta debiera proporcionarse después de ceder los datos. Esta idea se contradice con el hecho de que deba efectuarse «en el momento en que se efectúe la primera cesión de datos». Por otro lado, si posteriormente se llevan a cabo otras cesiones de datos del mismo afectado al mismo cesionario, ¿deberá cumplirse también este deber? ¿Y si se realizan estas cesiones a otro cesionario? Pero es que además, como ya se ha indicado anteriormente, para que el consentimiento sea válido para ceder datos no es necesario identificar al cesionario. En cambio, este artículo 27 sí exige la identificación. ¿Por qué esta exigencia mayor de información?

Hay que decir que este artículo ha sido prácticamente ignorado. A ello ha contribuido, además de su complejidad, la falta de tipificación adecuada en la ley para posibilitar su sanción hasta el cambio en el régimen del marco sancionador que se llevó a cabo en el año 2011[5].

[(5)]Modificación de los artículos 43, 44, 45, 46 y 49 LOPD, introducida por la Ley 2/2011 de 4 de marzo de economía sostenible (BOE núm. 55, de 5 de marzo de 2011, págs. 25.033-25.235) (Durán, 2016, págs. 467-472).

Otra regulación especial que hay que tener en cuenta es la de los datos especialmente protegidos, contenida en los artículos 7 y 8 LOPD. Estos datos son los que revelen la ideología, afiliación sindical, religión y creencias, los que hagan referencia al origen racial, a la salud y a la vida sexual, así como los relativos a la comisión de infracciones penales o administrativas. Para poder ceder este tipo de datos deberá atenderse a estos preceptos (art. 10.5 RLOPD).

Esto implica que los datos que revelen la ideología, afiliación sindical, religión y creencias solo podrán cederse si se cuenta con el consentimiento expreso y por escrito del afectado (art. 7.2 LOPD). Los datos referidos al origen racial, a la salud y a la vida sexual solo podrán cederse cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente (art. 7.3 LOPD).

Asimismo, también hay que tener en cuenta que podrán tratar los datos de salud las instituciones, centros sanitarios y profesionales del sector (arts. 8 LOPD y 10.5 RLOPD) y la posibilidad que se contemplaba en la regulación general relativa a este mismo tipo de datos de salud de poder cederlos, si ello fuera

necesario para solucionar una urgencia que requiriera acceder a un fichero, o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad (art. 11.2.f) LOPD).

1.4. La cesión en el RGPD

El RGPD, al igual que la Directiva 95/46/CE, no incluye ninguna regulación especial para la cesión de datos, sino que lo trata como un tratamiento más.

De esta forma, es tratamiento la «comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión» (art. 4.2 RGPD). En consecuencia, se le aplicará a este tipo de operaciones la misma regulación general que a cualquier tratamiento de datos.

No obstante, y como también sucedía en la Directiva 95/46/CE, el RGPD se refiere a las comunicaciones pero no en una regulación completa específica, sino en algunas disposiciones.

En este sentido, se puede mencionar la definición de destinatario, que es la:

> «persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento» (art. 4.9 RGPD).

Según esta definición, la existencia del destinatario implica que habrá una comunicación de datos. Para tener una visión total de los sujetos que podrían ser destinatarios, hay que completar el concepto con el de tercero que se define como:

> «persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado» (art. 4.10 RGPD).

De la lectura de ambas definiciones se deduce que la comunicación de datos podrá realizarse a sujetos que puedan ser terceros o no. Es decir, que la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos, que será considerado destinatario, podría ser el encargado o las personas autorizadas para tratar los datos bajo la autoridad del responsable o del encargado.

En virtud de estos conceptos cabe plantearse si las transmisiones de datos que se realizan a encargados, o incluso a empleados del responsable o del encargado, deben someterse a la regulación general. Es decir, por ejemplo, cabe plantear si el responsable debe hallar la base legal del artículo 6 RGPD que legitime estas comunicaciones de datos.

Si bien podremos encontrar una base legal que permita estas comunicaciones (el mismo RGPD nos dará las herramientas), de entrada, lo cierto es que esta interpretación chocaría con la concepción tradicional de nuestra LOPD. Y es que, en la LOPD, el encargo del tratamiento se consideraba que no era una comunicación, de forma que evitaba la aplicación de la regulación específica sobre este tratamiento.

Pero ¿cuál fue el objetivo de introducir esta figura de destinatario? Para ello, debemos acudir al proceso de elaboración de la Directiva 95/46/CE, antecedente del RGPD, que introdujo esta figura prácticamente con la misma definición del RGPD[6]. Así comprobamos que este concepto se incluyó en la versión final de la Directiva 95/46/CE directamente, a iniciativa de la delegación francesa y de la Comisión, que propusieron deslindar esta noción de la de tercero (Heredero, 1997, pág. 82). La explicación para hacerlo fue «que es útil para garantizar la transparencia de los tratamientos con respecto a las personas afectadas»[7].

Referencia bibliográfica

M. Heredero (1997). *La Directiva comunitaria de protección de los datos de carácter personal (Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales*. Cizur Menor: Aranzadi.

(6)Así, el destinatario se define en la Directiva 95/46/CE como «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios» (art. 2.g) Directiva 95/46/CE).

(7)Posición común (CE) núm. 1/95 adoptada por el Consejo el 20 de febrero de 1995 con vistas a la adopción de la Directiva 95/…/CE del Parlamento Europeo y del Consejo, de …, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO C 93 de 13 de abril de 1995, apdo. 2.i..

Por tanto, la única finalidad por la que se introdujo este concepto de destinatario en la Directiva 95/46/CE fue para incrementar la transparencia en el tratamiento de datos de cara al interesado[8].

(8)Durán, 2016, pág. 369.

De la misma forma, el destinatario aparece principalmente en los preceptos que el RGPD dedica a establecer obligaciones informativas. Así, tanto en la información que el responsable debe facilitar cuando obtenga los datos del interesado como cuando los obtenga de otra fuente figuran los destinatarios (arts. 13.1.e y 14.1.e RGPD). En el caso de recogida indirecta de datos, se añade la necesidad de informar de la intención de «transferir datos personales a un destinatario en un tercer país» (art. 14.1.f RGPD).

El responsable debe informar también de los destinatarios, incluso los que estén en terceros países en caso de que el interesado ejerza su derecho de acceso (art. 15.1.c RGPD). Asimismo, aparece el término destinatario en la obligación

de notificación que tiene el responsable a aquellos sujetos a los que hubiera comunicado datos personales, en caso de que los afectados hubieran ejercido los derechos de rectificación, supresión o limitación del tratamiento (art. 19 RGPD). También el responsable debe incluir en el registro de las actividades de tratamiento las categorías de destinatarios a quienes se comuniquen los datos (art. 30.1.d RGPD).

Hay que añadir que la definición establece que las autoridades públicas no deben considerarse destinatarios, lo que implicará por lo tanto que no deberá informarse a los afectados sobre estas cesiones de datos. Sin embargo, estos casos se limitan, ya que debe tratarse de comunicaciones a autoridades públicas en virtud de una obligación legal para que estas ejerzan su misión oficial de investigación, como puede ser en el caso de las autoridades fiscales y aduaneras, las unidades de investigación financiera, autoridades administrativas independientes u organismos de supervisión de los mercados financieros. Además, en estos casos, las solicitudes de comunicación por parte de estas autoridades deben realizarse por escrito, de forma motivada, deben ser ocasionales y no referirse a la totalidad de un fichero ni suponer interconexión de varios ficheros (Considerando 31 RGPD).

Observamos algunas alusiones que se hacen en el RGPD a la comunicación de datos que comentamos a continuación, también principalmente con la intención de limitar o ampliar el deber de informar que tiene el responsable del tratamiento.

Así, como en la Directiva 95/46/CE, en la recogida indirecta se excepciona la obligación de informar de los aspectos previstos si la comunicación de datos está expresamente establecida en la legislación aplicable al responsable del tratamiento (art. 14.5.c RGPD).

Una obligación informativa que no estaba en la Directiva 95/46/CE, referida a la comunicación y no al destinatario, es la que se establece cuando la recogida de datos sea directa consistente en indicar si la comunicación de datos que pueda realizarse es un requisito legal o contractual o necesario para suscribir un contrato y si el interesado está obligado a facilitar los datos y está informado de las consecuencias de no hacerlo (art. 13.2.e RGPD).

Un límite temporal de la obligación de informar en la recogida indirecta, que también incluía la Directiva 95/46/CE, alude en el RGPD a la comunicación. De esta forma, cuando se tenga previsto comunicar datos a un destinatario, se debe proporcionar la información al interesado a más tardar en el momento de la primera comunicación a este destinatario (art. 14.3.c RGPD).

Otra referencia a un supuesto de cesión de datos es cuando el RGPD, al igual que la Directiva 95/46/CE, habilita la posibilidad de tratar datos para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un

tercero (art. 6.1.f RGPD), de manera que este último caso implica necesariamente que existirá una comunicación de datos a ese tercero. No obstante, en este caso la cesión es a un tercero, no a un destinatario.

Las transferencias internacionales conllevan también la existencia de comunicaciones de datos a otros sujetos. Específicamente, en el marco de las transferencias internacionales se incluye el artículo 48 con la rúbrica «transferencias o comunicaciones no autorizadas por el derecho de la Unión». Este artículo pretende evitar que un responsable o un encargado comuniquen o transfieran datos por exigencia de una sentencia de un órgano jurisdiccional o una decisión de una autoridad administrativa de un tercer país, excepto si son reconocidas o ejecutables en virtud de un acuerdo internacional[9] (Durán, 2016, pág. 696).

(9)La introducción de este precepto respondió a la alarma generada durante el procedimiento legislativo al desvelarse el alcance de los programas de espionaje del gobierno de Estados Unidos, de forma que se pretendía limitar la posibilidad de que se accediera a datos de los ciudadanos europeos sin las debidas garantías.

En conclusión, sin perjuicio de futuras interpretaciones que aclaren el papel del destinatario en el RGPD, hay que entender que tiene una finalidad eminentemente informativa y, por ello, se amplía al encargado del tratamiento y a las personas bajo la autoridad del responsable y del encargado. No obstante, esto no obligaría a aplicar la regulación general de los tratamientos a esta transmisión de datos. Y es que, como veremos a continuación, el encargado (al igual que hacen los empleados del responsable y del encargado) realizará el tratamiento de datos por cuenta del responsable y de acuerdo con los requisitos que el mismo RGPD dispone. Por ello, la legitimación de la comunicación de datos al encargado, si es el caso, debe conectarse con la posibilidad que brinda el RGPD de que el responsable encomiende a otros los tratamientos. El responsable del tratamiento debe analizar si cuenta con una base legal para efectuar estos tratamientos que llevará a cabo el encargado o los empleados. Esto es, si el responsable del tratamiento cuenta con una base legal que le habilita al tratamiento de datos personales no es preciso que busque otra base legal para que el encargado del tratamiento pueda llevarlo a cabo.

2. El encargado del tratamiento

La figura del encargado del tratamiento se incluyó en la Directiva 95/46/CE, de forma que completaba la protección que otorgaba esta norma, al alcanzar también el tratamiento de datos personales que realizaban los proveedores de servicios para los responsables. En la legislación española se ha construido una regulación sobre esta figura que ha tenido claramente influencia en la establecida por el RGPD. De esta forma, en el RGPD, en contraste con la regulación contenida en la Directiva 95/46/CE, se ha ampliado el catálogo de obligaciones asignadas a este sujeto y se le ha atribuido una clara responsabilidad, de forma que puede ser sancionado si incumple estos deberes.

2.1. El encargado del tratamiento: definición y distinción del responsable

2.1.1. La definición de encargado del tratamiento

El encargado del tratamiento se define como «la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento» (art. 4.8 RGPD). El rol de encargado del tratamiento se adjudicaría a aquel prestador de servicios que contrate el responsable, que requiera, para poder realizar el servicio contratado, llevar a cabo un tratamiento de datos personales.

Tanto en la Directiva 95/46/CE como en la LOPD se incluía esta misma definición, aunque en la LOPD se añadía la posibilidad de que el encargado actuara solo o conjuntamente con otros. Esta definición se ampliaba en el RLOPD 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» (art. 5.1.i RLOPD).

Como vemos, no se incluye en el RGPD la especificación relativa a la existencia de una relación jurídica previa que delimita el ámbito de actuación del encargado para la prestación de un servicio, ni tampoco se habilita la posibilidad de que sean encargados los entes sin personalidad jurídica. Quedará por tanto la duda sobre si es necesario, para calificar un sujeto como encargado, que lleve a cabo un servicio y si es posible que este carezca de personalidad jurídica.

En cuanto a la relación entre el responsable y el encargado del tratamiento, en la definición que proporciona el RLOPD se hace referencia a que el encargado trata los datos por cuenta del responsable como consecuencia de una prestación de servicios y eso delimita ya el encargo. En cambio, el RGPD no especifica esto, sino que lo que hace es obligar a que encargado y responsable suscriban un contrato de acuerdo con lo estipulado en el mismo RGPD.

Por tanto, la definición de encargado tendría un elemento subjetivo, que sería «la persona física o jurídica, autoridad pública, servicio u otro organismo», y un elemento objetivo, que sería el tratamiento de datos, pero lo que caracteriza al encargado del tratamiento es que realiza el tratamiento «por cuenta» del responsable, mientras que el responsable es el que «determina los fines y medios del tratamiento» (art. 4.7 RGPD). En consecuencia, cuando un sujeto determine los fines y medios del tratamiento, no podrá ser considerado encargado del tratamiento sino responsable del tratamiento.

Si bien el término «fines» parece claro, ¿qué debe entenderse por «medios del tratamiento»? A falta de pautas específicas de las autoridades de protección de datos sobre el RGPD, y dada la práctica identidad con el texto de la Directiva 95/46/CE, cabe acudir a la interpretación que realizó el Grupo del Artículo 29 (GA29) sobre este término.

De acuerdo con esta interpretación, los medios se referirían a: a) los medios técnicos y organizativos utilizados para realizar el tratamiento, b) la determinación de los datos, c) las operaciones a realizar y e) los terceros que tendrán acceso a los datos. Ahora bien, solo la determinación de los fines y la de los medios considerados esenciales será la que activaría el rol de responsable[10] (Durán, 2016, pág. 138).

(10)Grupo de Trabajo Artículo 29, 2010.

Los medios esenciales serán todos los mencionados, excepto los medios técnicos y organizativos (como son el software o el hardware que se utilicen). Esto permitirá que el encargado del tratamiento pueda elegir los medios técnicos que quiere utilizar para llevar a cabo el tratamiento, y ello no implicará que se convierta en responsable.

Ahora bien, cabe plantearse si las medidas de seguridad serían un elemento esencial de los medios[12]. El RGPD dispone que la obligación de aplicar medidas organizativas y técnicas para garantizar un nivel adecuado al riesgo la deben cumplir el responsable y el encargado (art. 32.1 RGPD). Además, en el contrato que deben suscribir ambos sujetos debe constar que el encargado adoptará estas medidas de seguridad (28.3.c RGPD). Pero ¿esto implica que el encargado determinará qué medidas de seguridad aplica de forma autónoma? ¿O debe ser el responsable el que establezca estas medidas que debe adoptar el encargado? Las autoridades de protección de datos españolas han indicado que de-

(11)Agencia Española de Protección de Datos, Autoritat Catalana de Protecció de Dades, Agencia Vasca de Protección de Datos, pág. 7.

ben establecerse estas medidas de seguridad en el contrato, sin concretar de quién es la obligación de determinación de las mismas. Estas medidas pueden incorporarse en una lista exhaustiva o realizar una remisión a un estándar o a un marco nacional o internacional reconocido[11].

(12)El GA29 consideraba, en el marco de la Directiva 95/46/CE, que no eran un elemento esencial de los medios, pero reconocía que en algunas legislaciones nacionales como la italiana sí tenían ese carácter. En la legislación española también se podía entender que eran un elemento esencial, ya que era el responsable del tratamiento el que debía indicar al encargado en el contrato que debían suscribir las medidas de seguridad que este último debía adoptar.

2.1.2. La distinción entre el encargado y el responsable

La distinción entre el responsable y el encargado siempre ha sido una cuestión harto compleja e importante, ya que supone la aplicación de preceptos diferentes. Una forma de analizar si estamos ante un sujeto u otro es hallar de dónde emana el poder de determinación de los fines y los medios esenciales del tratamiento. Si encontramos esta fuente, quiere decir que el sujeto que estamos analizando debe considerarse responsable. En caso de no hallar la fuente del poder de determinación, podremos analizar si debemos calificar al sujeto como encargado por cumplirse los elementos de su definición.

Entre estas posibles fuentes del poder de determinación tenemos la ley, que podría establecer claramente que el sujeto analizado fuera un responsable o un encargado, o darnos indicios para poder llegar a esta conclusión[13]. El sujeto analizado puede estar sometido a obligaciones legales que impliquen que deba gozar de una cierta autonomía en su actuación respecto al tratamiento de datos. Esta autonomía podría conllevar que tuviera que determinar los fines o los medios esenciales del tratamiento y, por tanto, que tuviera que ser considerado responsable. Esta autonomía también puede derivarse de obligaciones deontológicas propias de las profesiones reguladas.

(13)Un ejemplo de determinación legal del responsable es la Ley de mediación de seguros y reaseguros privados. En esta ley se establece una sección dedicada a la protección de datos, en la que califica como responsables a los corredores de seguros y como encargados de las compañías a los agentes de seguros. Artículo 62 Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros (BOE núm. 170, 18 de julio de 2006).

El GA29 mencionaba, como un criterio que podía ser tenido en cuenta para determinar si un sujeto debía ser calificado de responsable o de encargado, el relativo a los conocimientos especializados que debía tener el prestador de servicios[14]. Así, un prestador de servicios que deba reunir estos conocimientos no sería lógico que debiera seguir las instrucciones del cliente. En definitiva, los ejemplos que cita el GA29 respecto a este criterio son los de profesiones fuertemente reguladas, como son los abogados, que deben ostentar una independencia respecto a sus clientes, por más que trabajen para estos.

(14)Grupo de Trabajo Artículo 29, 2010, pág. 32.

Además de acudir a la legislación, el poder de determinación también podría emanar de la relación contractual existente entre responsable y encargado. No obstante, el GA29 ha interpretado que el contrato no debe ser un aspecto decisivo ni constitutivo para establecer si estamos ante un encargado o no[15]. De esta forma, para el GA29 es más importante la realidad que lo que se refleje en un contrato. De este modo se ha querido evitar que se creen relaciones de responsable y encargado artificiosas, que lo único que pretendan sea eludir la regulación que regiría si no se pudiera aplicar la figura del encargo.

(15)Grupo de Trabajo Artículo 29, 2010, pág. 30.

En esta realidad se podrán encontrar indicios que ayuden a establecer si un sujeto tiene o no poder de determinación de los fines y medios del tratamiento como, por ejemplo, el nivel de instrucciones que proporcione el responsable y que determinará el margen de maniobra que le quedará al encargado, o el seguimiento que el responsable realice de la ejecución del servicio, de forma que si realiza una supervisión estricta mostrará un control pleno por parte del mismo sobre el tratamiento[16]. Otro indicio será la visibilidad o la imagen que tengan los interesados sobre quién es el responsable.

(16)Grupo de Trabajo Artículo 29, 2010, págs. 31-34.

2.2. La relación contractual entre responsable y encargado del tratamiento

Antes de suscribir el contrato, el responsable debe elegir al encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para cumplir con el RGPD y proteger los derechos de los interesados (art. 28.1 RGPD). Este deber de diligencia *in eligendo* ya se establecía en la Directiva 95/46/CE y en el RLOPD[17]. Estas garantías suficientes podrán demostrarse con el cumplimiento de códigos de conducta o mecanismos de certificación (art. 28.5 RGPD).

(17)«Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento» (art. 20.2 RLOPD). La Directiva 95/46/CE, en su artículo 17.2, contemplaba la necesidad de que los Estados miembros establecieran esta obligación para el responsable del tratamiento de elegir al encargado que reúna las garantías suficientes para cumplir las medidas de seguridad y se añadía que debía asegurar que se cumplieran estas medidas. Por tanto, la Directiva 95/46/CE también se refería a la responsabilidad *in vigilando* del responsable sobre el encargado. En este sentido, el TJUE ha indicado que «de los artículos 16 y 17 de la Directiva 95/46/CE, en los cuales se especifica el nivel de control que ejercerá en cada caso el responsable del tratamiento sobre el encargado que seleccione, se desprende que este último solo actuará cuando se lo encargue el responsable del tratamiento y que el responsable se asegurará de que se cumplan las medidas acordadas para proteger los datos personales contra cualquier tratamiento ilícito». Sentencia del TJUE, de 22 de noviembre de 2012, Probst, C-119/12, EU:C:2012:748, apdo. 25.

Una vez el responsable ha seleccionado el encargado, debe suscribir con él un contrato u otro acto jurídico que, con arreglo al derecho de la Unión o de los Estados miembros, le vincule y que debe constar por escrito. La posibilidad de que el tratamiento se rija por este acto jurídico distinto a un contrato será una novedad para nosotros, ya que la LOPD solo contemplaba el contrato.

(18)Agencia Española de Protección de Datos, Autoritat Catalana de Protecció de Dades, Agencia Vasca de Protección de Datos).

Este acto jurídico deberá establecer y definir la posición del encargado del tratamiento y podría ser, por ejemplo, una resolución administrativa notificada al encargado[18].

El contrato o acto jurídico debe establecer el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados y las obligaciones y derechos del responsable. Asimismo, debe estipular las obligaciones del encargado del tratamiento, señaladas por el artículo 28.3 RGPD, que a continuación analizamos:

1) Seguir las instrucciones del responsable

El encargado debe tratar los datos únicamente siguiendo instrucciones documentadas del responsable, salvo que esté obligado a ello en virtud del derecho de la Unión o de los Estados miembros que se aplique al encargado. En este caso, el encargado debe informar al responsable de esa exigencia legal, salvo que se prohíba por razones importantes de interés público.

2) Deber de confidencialidad

El encargado ha de garantizar que las personas autorizadas para tratar datos se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad estatutaria.

3) Medidas de seguridad

El encargado debe adoptar las medidas de seguridad según indica el artículo 32 RGPD. Este precepto adopta un enfoque orientado al riesgo, de forma que las medidas técnicas y organizativas que deben adoptarse serán las apropiadas para garantizar un nivel adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas (art. 32.1 RGPD).

Se ofrecen unas pautas acerca de los riesgos que un tratamiento puede suponer para los derechos y libertades de las personas físicas en el preámbulo, especialmente en el extenso Considerando 75 RGPD, que se reproduce parcialmente a continuación:

> «Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo» (Considerando 75 RGPD).

A esto se añade que, para evaluar si el nivel de seguridad es el adecuado, el artículo 32.2 RGPD indica que se deben tener en cuenta los riesgos que presente el tratamiento y se menciona como posibles causas de los mismos: la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Estos riesgos pueden revestir una gravedad o probabilidad variables, factores que serán los que deberán determinarse en función de la naturaleza, el alcance, el contexto y los fines del tratamiento[19].

[19]La gravedad y la probabilidad son factores de lo que es una metodología típica de un análisis de riesgos que tiene en cuenta el impacto y la probabilidad de que se produzca una amenaza, en concreto, que pueda afectar a lo que se protege, en este caso, los derechos y libertades, que sería el activo protegido.

En referencia al enfoque adoptado de riesgos, el GA29 alertó sobre la visión errónea que parecía extenderse sobre esta metodología de que podía ser una alternativa a los derechos y principios de protección de datos, en vez de una manera de adaptar el cumplimiento de forma que fuera escalable[20]. Por eso, el GA29 publicó un manifiesto en el que recordó que el derecho a la protección de datos es un derecho fundamental y cualquier operación de tratamiento debía respetarlo[21]. Los derechos que la ley brinda a los titulares de datos personales debían ser respetados, independientemente del nivel de riesgo que pudiera afectar al tratamiento de datos.

[20]Article 29 Data Protection Working Party, 2014, pág. 2.

[21]Article 29 Data Protection Working Party, 2014, pág. 3.

Entre las medidas técnicas y organizativas que el responsable o el encargado deberán adoptar se incluyen, como un listado no exhaustivo, las siguientes:

«**a)** la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento (art. 32.1 RGPD).»

Fruto de la incentivación de la autorregulación, se ha previsto la posibilidad de utilizar códigos de conducta y mecanismos de certificación para demostrar el cumplimiento de esta obligación (art. 32.3 RGPD).

El encargado debe adoptar las medidas que garanticen que cualquier persona que actúe bajo su autoridad y que tenga acceso a los datos los trate de acuerdo con las instrucciones del responsable del tratamiento, salvo si está obligada en virtud del derecho de la Unión o de los Estados miembros (art. 32.4 RGPD).

4) Subcontratación

El encargado deberá respetar las condiciones relativas a la subcontratación, es decir, que deberá contar con la autorización previa por escrito del responsable. Esta autorización podrá ser específica o general. En caso de que sea general la autorización, el encargado deberá informar cuando quiera contratar nuevos encargados o quiera sustituir a los existentes, de forma que el responsable pueda oponerse a estos cambios. El encargado deberá imponer a estos otros encargados, también mediante contrato o acto jurídico, establecido de acuerdo con el derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato o acto jurídico suscrito entre el responsable y el encargado.

5) Atención de derechos y ayuda al responsable en el cumplimiento de sus obligaciones

El encargado ha de asistir al responsable mediante medidas técnicas y organizativas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes de ejercicio de los derechos de los interesados.

Además, el encargado debe ayudar al responsable a garantizar el cumplimiento de sus obligaciones relativas a la seguridad, a la notificación de violaciones de la seguridad, a la evaluación de impacto y a la consulta previa a las autoridades de control.

6) Finalización del servicio

A elección del responsable, el encargado deberá suprimir o devolver todos los datos personales una vez finalice la prestación de los servicios del tratamiento y suprimir las copias existentes a menos que se requiera la conservación de los datos personales en virtud de la legislación aplicable.

7) Proporcionar evidencias de cumplimiento

Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de estas obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por el responsable.

Para facilitar la elaboración de estos contratos, tanto la Comisión como las autoridades de control podrán adoptar cláusulas contractuales tipo. En este sentido, las agencias de protección de datos españolas, durante el plazo transitorio de preparación para cumplir el RGPD, publicaron unas directrices para la elaboración de los contratos entre responsables y encargados del tratamiento[22]. Aunque las agencias dejaron claro que no constituían cláusulas tipo según lo indicado en el RGPD, en este documento se incluyó un modelo de cláusulas contractuales para facilitar la adaptación de los contratos al cumplimiento del RGPD durante la fase de preparación.

[22]Agencia Española de Protección de Datos, Autoritat Catalana de Protecció de Dades, Agencia Vasca de Protección de Datos.

2.3. Las obligaciones del encargado del tratamiento

Además de las obligaciones que hemos visto que tiene el encargado del tratamiento y que deben establecerse expresamente en el contrato que ha de suscribir con el responsable, debemos hacer mención a otras obligaciones que acaban de conformar su estatuto y que se encuentran principalmente en el capítulo IV, dedicado al responsable y al encargado del tratamiento, así como aquellas derivadas de la regulación de las transferencias internacionales ubicadas en el capítulo V del RGPD. Las que hallamos en el capítulo IV serían: la designación del delegado de protección de datos y del representante, el registro de las actividades del tratamiento, la notificación de violaciones de la seguridad de los datos, el deber de confidencialidad y la cooperación con la autoridad de control.

2.3.1. Designación del delegado de protección de datos

La Directiva 95/46/CE establecía la posibilidad de que los Estados miembros incorporaran en su legislación la figura del denominado encargado de protección de datos personales (art. 18 Directiva 95/46/CE). Con la designación de este encargado, se podía eliminar o simplificar la obligación de notificación de los tratamientos a la autoridad de control. El legislador español no incorporó la figura.

El RGPD la retoma y la denomina delegado de protección de datos (DPD) otorgándole mayor relevancia, ya que su designación deviene obligatoria en los supuestos establecidos.

El encargado del tratamiento (y también el responsable) debe designarlo en los siguientes casos, cuando:

> «**a)** el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
>
> **b)** las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
>
> **c)** las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10» (art. 37.1 RGPD).

Respecto al primer supuesto (a) la definición de lo que se considere autoridad u organismo público se deja al derecho interno, aunque el GA29 indicó como buena práctica que, aunque sean entidades privadas las que lleven a cabo la gestión de servicios públicos o que ejerzan potestades públicas, designen al DPD[23].

(23)Article 29 Data Protection Working Party, 2017, pág. 6.

Respecto al segundo supuesto de designación obligatoria (b) los siguientes términos plantean dudas acerca de su significado: «actividades principales», «observación habitual y sistemática» y «a gran escala».

En el Considerando 97, el RGPD indicaba que las actividades principales de un responsable estarán relacionadas con sus actividades primarias, no con el tratamiento de datos como actividad auxiliar. El GA29 indicó que, por ejemplo, un hospital cuya actividad principal es claramente la atención sanitaria debería nombrar un DPD, ya que el tratamiento de datos de sus pacientes también debe considerarse actividad principal al estar la atención sanitaria inextricablemente unida al tratamiento de datos[24].

(24)Article 29 Data Protection Working Party, 2017, pág. 7.

La noción de «observación habitual y sistemática», según el GA29, incluiría la monitorización que se realiza en internet con fines de publicidad orientada al comportamiento, aunque también precisa que no debe limitarse al entorno en línea.

El término «habitual», para el GA29, implica uno o más de los siguientes supuestos:

- Que ocurre en intervalos concretos en un período determinado.
- Que es recurrente o que se repite en momentos concretos.
- Que se produce de forma constante o periódica.

El término «sistemática» significa uno o más de los siguientes supuestos:

- Que ocurre de acuerdo con un sistema.
- Es planificado, organizado o metódico.
- Tiene lugar como parte de un plan general para recoger datos.
- Se lleva a cabo como parte de una estrategia.

Como ejemplos de actividades que constituyen una observación habitual y sistemática, el GA29 mencionó: los servicios de telecomunicaciones, de *scoring* y de creación de perfiles, los de monitorización de la ubicación como algunas *apps*, programas de fidelización, de monitorización de salud o ejercicio físico a través de dispositivos o los servicios proporcionados a través de dispositivos conectados (Internet of Things)[25].

(25)Article 29 Data Protection Working Party, 2017, pág. 9.

Para determinar si un tratamiento se realiza «a gran escala», el GA29 recoge factores a los que apunta el Considerando 91 cuando se refiere a las evaluaciones de impacto[26]. Así se refiere al número de afectados, al volumen de datos

(26)Article 29 Data Protection Working Party, 2017, pág. 7 a 8.

tratados y a la tipología de datos, a la duración y permanencia de la actividad del tratamiento y al ámbito geográfico de la misma. El GA29 menciona, como ejemplos de observación a gran escala, el tratamiento de datos de pacientes en un hospital, o el de datos del transporte de personas que utilizan un servicio público o el de datos de clientes de bancos o compañías de seguros.

Respecto al tercer supuesto de designación obligatoria (c), de nuevo habrá que acudir a la interpretación de la noción de «a gran escala», pero esta vez el tratamiento debe ser de las llamadas categorías especiales de datos. Estos datos son los que, en la legislación española, se conocían como datos especialmente protegidos, aunque en el RGPD se ha ampliado la tipología, de forma que incluirían: datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical; datos genéticos, biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física. A estos datos hay que añadir los relativos a condenas e infracciones penales que también obligarán al nombramiento del DPD.

En otros casos diferentes a los mencionados, se puede nombrar al delegado y se deja abierta la posibilidad de que los Estados miembros o el derecho de la Unión obliguen a su designación (art. 37.4 RGPD). Por otro lado, se permite que se pueda nombrar un único delegado en un grupo empresarial y en una Administración pública para varias autoridades u organismos (art. 37.2 y 3 RGPD).

El delegado rendirá cuentas directamente al más alto nivel jerárquico del responsable o del encargado (art. 38.3 RGPD). Asimismo, la designación del delegado responde al objetivo de transparencia, de forma que se exige la comunicación de la designación a la autoridad de control y al público (art. 37.7 RGPD). Además, se establece la posibilidad de que los interesados puedan contactar con el delegado en todo lo relativo al tratamiento de sus datos personales y al ejercicio de sus derechos (art. 38.4 RGPD).

El RGPD indica que la designación del DPD debe realizarse atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones que se establecen en el reglamento (art. 37.5 RGPD).

El GA29 mencionó que el nivel de conocimientos debe valorarse en virtud de la sensibilidad, complejidad y volumen de datos que la organización procese[27]. También debe tenerse en cuenta si la entidad realiza transferencias internacionales sistemáticamente o solo de forma ocasional. Respecto a las cualidades profesionales, es relevante que conozca las legislaciones europeas y nacionales de protección de datos y especialmente en profundidad el RGPD. Debe valorarse el conocimiento del sector de negocio, así como de la organi-

(27)Article 29 Data Protection Working Party, 2017, pág. 11.

zación del responsable o encargado. El DPD debería conocer suficientemente las operaciones del tratamiento, los sistemas de información y las necesidades de seguridad.

El GA29 puso de relevancia que el DPD debía poseer habilidades personales que incluyan la integridad y un alto grado de ética profesional, de forma que su primer objetivo sea el cumplimiento del RGPD.

En este sentido, la Agencia Española de Protección de Datos ha colaborado con la Entidad Nacional de Acreditación (ENAC) para elaborar un esquema de certificación para la acreditación de organismos de certificación de DPD.

El DPD puede ser un empleado del responsable o del encargado o puede ser un prestador de servicios externo. En este último caso, el GA29 indicó que es importante que el DPD pueda llevar a cabo sus funciones, tal como se establecen en el RGPD y a las que haremos mención posteriormente[28]. También debe estar protegida su independencia, al igual que sucede con el DPD interno.

(28)Article 29 Data Protection Working Party, 2017, pág. 12.

De la contratación externa del DPD, el GA29 resaltó que puede reunir las cualidades profesionales y conocimientos requeridos en un equipo de trabajo, en lugar de tener que recaer en una sola persona. Esto puede facilitar el alto nivel de especialización requerido. En este caso, el GA29 recomendaba que exista una clara definición de las tareas de este equipo y la asignación de una persona responsable para cada cliente, lo que podría incluirse en el contrato de servicios.

2.3.2. Designación de representante

En los casos en los que se aplique el reglamento a encargados que no están establecidos en la UE, según el criterio de aplicación establecido en el artículo 3.2 RGPD, estos encargados están obligados a designar a un representante. La definición de representante es:

> «Persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento, con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento» (art. 4.17 RGPD).

De acuerdo con esta definición, el representante no debería contar con obligaciones propias, sino que tendría las obligaciones que el RGPD estableciera para el responsable. Sin embargo, se le han asignado algunos deberes, especialmente dirigidos a la colaboración con las autoridades de control, ya que su principal función será atender las consultas de estas autoridades o de los interesados sobre el tratamiento de datos (art. 27.4 RGPD)[29]. Para ello, los datos del representante se incluyen entre la información que debe proporcionarse al interesado cuando se recojan sus datos (arts. 13.1.a y 14.1.a RGPD).

(29)Así, se cita expresamente al representante como sujeto obligado en el artículo 30.1 RGPD (obligación de registro de las actividades de tratamiento) y en el artículo 31 RGPD (cooperación con autoridades de control).

Este representante debe hallarse en uno de los Estados miembros donde residan los interesados cuyos datos son objeto del tratamiento, en los dos supuestos que activan la aplicación del reglamento, es decir: donde estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado (art. 27.3 RGPD).

Sin embargo, esta obligación de designar representante cuenta con algunas excepciones que se refieren a cuando el responsable o encargado fuera una autoridad u organismo público, o si el tratamiento fuera ocasional, no incluyera categorías especiales de datos ni datos de condenas o infracciones penales y fuera improbable que entrañara un riesgo para los derechos y libertades de las personas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento (art. 27.2 RGPD).

Si bien se mantiene la alusión que se hacía en la Directiva 95/46/CE a que la designación de este representante no obsta para que se puedan ejercitar las acciones legales contra el responsable o el encargado (art. 27.5 RGPD), se incluye en el preámbulo que el representante podría estar sujeto a medidas coercitivas, en caso de incumplimiento del responsable o del encargado (Considerando 80 RGPD).

2.3.3. Registro de las actividades del tratamiento

Esta obligación responde plenamente al principio de responsabilidad activa o *accountability*, de forma que su objetivo es que el responsable pueda demostrar que cumple con lo establecido en el reglamento frente a las autoridades de control. Por tanto, estamos ante una obligación formal y que implica la puesta a disposición, de esta documentación, a la autoridad de control (art. 30.4 RGPD).

Los sujetos obligados son el responsable y también el encargado, así como sus representantes. En el caso del encargado, el registro debe referirse a las actividades de tratamiento efectuadas por cuenta del responsable (art. 30.2 RGPD).

Durante el proceso legislativo del RGPD se redujo el alcance de la obligación que, inicialmente, exigía la conservación de la documentación de todas las operaciones del tratamiento y había incluido un mínimo de información que debía contener la documentación. Se trataba de un listado bastante amplio descriptivo de las operaciones y de todos los sujetos implicados. Finalmente, se redujo la información que debía registrarse que, en el caso del encargado es:

«**a)** el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1» (art. 30.2 RGPD).

Con el fin de simplificar los requisitos para las pymes, se ha previsto la excepción en la aplicación de esta obligación para empresas u organizaciones con menos de 250 empleados, a menos que el tratamiento pueda entrañar riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos personales de condenas e infracciones penales (art. 30.5 RGPD).

2.3.4. Notificación de violaciones de la seguridad de los datos

La incorporación de esta obligación supone la generalización de la misma para todos los responsables del tratamiento, ya que actualmente existe esta obligación, de forma sectorial, para los prestadores de servicios de comunicaciones electrónicas en el marco de la Directiva 2002/58/CE. Respecto a este deber de notificación sectorial, se aprobó un reglamento europeo con el fin de asegurar un procedimiento uniforme en toda la UE, para realizar la notificación[30].

[30]Reglamento (UE) núm. 611/2013, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas, DO L 173, de 26 de junio de 2013. En España, esta obligación se recoge en el artículo 41.3 Ley 9/2014, de 9 de mayo, general de telecomunicaciones (BOE núm. 114 de 10 de mayo de 2014) y la notificación se realiza a la AEPD a través de su sede electrónica.

En nuestra normativa nacional, debemos recordar la medida de seguridad que establecía el RLOPD referente al registro de incidencias que exigía la existencia de un procedimiento de notificación y gestión de estas incidencias (arts. 90 y 100 RLOPD). No obstante, este procedimiento era interno, por lo que no exigía la notificación a las autoridades de protección de datos.

La violación de la seguridad de los datos personales, se define como:

«toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos» (art. 4.12 RGPD).

La obligación de comunicar estas violaciones de seguridad contribuye a la transparencia en el tratamiento de datos de cara al interesado y permite que este pueda tener el control sobre lo que sucede con sus datos. No cabe duda de la relevancia que conlleva un fallo de seguridad en el contexto de internet, donde los datos pueden quedar expuestos a la vista de todo el mundo.

Se ha asignado la obligación al responsable, aunque el encargado también debe notificar al responsable las violaciones de seguridad de las que tuviera conocimiento sin dilación indebida (art. 33.2 RGPD).

2.3.5. Confidencialidad

El RGPD reitera el deber del encargado del tratamiento de tratar los datos únicamente siguiendo las instrucciones del responsable, a no ser que estén obligados a ello en virtud del derecho de la Unión o de los Estados miembros (art. 29 RGPD), obligación que ya hemos visto que se establecía entre los aspectos que debían incluirse en el contrato a suscribir entre encargado y responsable (art. 28.3.a RGPD). Este deber se amplía también a cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales.

2.3.6. Cooperación con la autoridad de control

El encargado, al igual que el responsable y sus representantes, deben cooperar con la autoridad de control que lo solicite en el desempeño de sus funciones (art. 31 RGPD).

2.3.7. Las obligaciones derivadas de la regulación de las transferencias internacionales de datos

El RGPD establece, como principio general, que el responsable y el encargado solo pueden realizar transferencias de datos personales a un tercer país o a una organización internacional si cumplen las condiciones establecidas en el capítulo V del Reglamento, en particular en lo tocante a las transferencias ulteriores (art. 44 RGPD).

Una de las diferencias más importantes que hay en el RGPD respecto a la Directiva 95/46/CE es que los sujetos que podrán transferir datos ya no son solo los responsables del tratamiento, sino que también podrán ser encargados del tratamiento. En este sentido, cabe mencionar que en España el concepto que el RLOPD establecía de exportador no especificaba si debía ser responsable o encargado, lo que respondió a la interpretación que había adoptado la AEPD para posibilitar que también el encargado pudiera iniciar el trámite de autorización para poder realizar transferencias internacionales (Durán, 2016, pág. 485).

Las posibilidades establecidas para que se permitan las transferencias a países terceros o a organizaciones internacionales se deben escoger de acuerdo con un orden de preferencia, lo que también es una novedad importante: la primera opción será que la Comisión Europea haya adoptado una decisión favorable a la adecuación del nivel de protección proporcionado por el país, un territorio o un sector del tratamiento de datos en ese país o la organización internacional (art. 45 RGPD); si no hay decisión de la Comisión, la segunda posibilidad es que el responsable o el encargado del tratamiento ofrezcan las garantías adecuadas (art. 46 RGPD) y, por último, si no se puede optar por ninguna de las dos anteriores, quedará que el supuesto se encaje en alguna de las excepciones que permitirán realizar la transferencia (art. 49 RGPD).

Las garantías que pueden ofrecer el responsable o el encargado para realizar las transferencias, en la segunda opción señalada, las podemos dividir, entre las que no requieren de autorización de la autoridad de control y las que sí. Las que no requieren autorización son las siguientes: un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos, las normas corporativas vinculantes o *binding corporate rules*, cláusulas tipo de protección de datos adoptadas por la Comisión, cláusulas tipo adoptadas por una autoridad de control y aprobadas por la Comisión y un código de conducta o un mecanismo de certificación aprobados de acuerdo con lo establecido en el RGPD, junto con compromisos vinculantes y exigibles (art. 46.2 RGPD). Como garantías que requieren de autorización de la autoridad de control, se establecen: cláusulas contractuales entre responsable o encargado y responsable, encargado o destinatario o disposiciones que se incorporen en acuerdos administrativos entre la autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados (art. 46.3 RGPD).

Se incluye en los textos la regulación detallada de la aprobación de las normas corporativas vinculantes que se definen como:

> «las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta» (art. 4.20 RGPD).

Entre los aspectos contemplados en esta regulación, dentro del contenido mínimo que debe constar en las normas, se exige la aceptación del responsable o del encargado europeos de la responsabilidad, por cualquier violación de las normas corporativas, por parte de cualquier miembro que no esté establecido en la UE (art. 47.2.f) RGPD). El responsable o el encargado solo podrán ser exonerados si prueban que el acto que originó el daño no es imputable a dicho miembro.

Respecto a las excepciones, que permitirían las transferencias, se mantienen las incluidas en la Directiva 95/46/CE, aunque se han introducido algunas precisiones[31]. No se contempla específicamente si puede aplicarlas el responsable o el encargado, salvo las que expresamente aluden al responsable, como las que se refieren a contratos entre el interesado y el responsable o a contratos en beneficio del interesado, cuya transferencia se realiza entre el responsable y otra persona. Esto da pie a plantear si es adecuado, en función del rol que ejerce el encargado, poder acudir a estas excepciones y, por ejemplo, solicitar consentimiento al interesado para poder realizar una transferencia.

[31]Así, por ejemplo, se exige que el consentimiento del interesado sea explícito y para obtenerlo deberá informarse de los riesgos que entraña la transferencia debido a la ausencia de decisión de adecuación y de garantías apropiadas (art. 49.1.a RGPD).

El hecho de que el encargado realice una transferencia en virtud de una base legal que determine él mismo, supondría que determinaría los fines del tratamiento y, por tanto, debería calificarse como responsable. Y es que el RGPD, al otorgar un papel tan relevante al encargado, no deja claro quién debe tener el control sobre el tratamiento (Durán, 2016, pág. 787).

2.4. Responsabilidad del encargado

Si el encargado del tratamiento infringe el RGPD, al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento (art. 28.10 RGPD). Esta fórmula de atribución de responsabilidad es algo diferente de la que se había establecido en la LOPD, que convertía al encargado en responsable si no seguía las instrucciones del responsable (art. 12.4 LOPD). La opción del RGPD se aleja de la desobediencia como criterio para atribuir esa responsabilidad al encargado, lo que es lógico si tenemos en cuenta que el mismo RGPD permite esta desobediencia del encargado si es debida al cumplimiento de obligaciones legales. Por tanto, el legislador europeo prefirió activar la responsabilidad del encargado cuando determinara los fines y los medios del tratamiento, algo que le estaría vetado al encargado, independientemente de si ello viene originado por la desobediencia respecto de aquello indicado por el responsable o no.

En caso de subcontratación, el RGPD atribuye al encargado principal la responsabilidad respecto al incumplimiento del subencargado de sus obligaciones de protección de datos (art. 28.4 RGPD).

Otro aspecto que ya se reflejaba en la Directiva 95/46/CE, respecto al encargado y a las personas sometidas a la autoridad del responsable y del encargado, era la posibilidad de desviarse del encargo del responsable cuando un imperativo legal así lo dispusiera. Como ya hemos visto, esta vía de escape también se ha previsto en el RGPD (art. 29 RGPD) y se ha reforzado para el encargado del tratamiento al indicar que seguirá las instrucciones del responsable, a menos que la legislación exija lo contrario (art. 28.3.a RGPD). Esta regulación se completa de forma que, en caso de que el encargado debiera actuar en virtud

de una obligación legal, tendría que informar al responsable de esta exigencia, salvo si la disposición legal le prohibiera dicha información por motivos importantes de interés público.

La utilización de esta vía para no atender las instrucciones del responsable plantea la duda de si implicaría que se pueda aplicar la activación mencionada de la responsabilidad del encargado[32]. Sin embargo, como la activación de esta responsabilidad presupone un incumplimiento del RGPD, en este caso, que respondería precisamente a lo establecido en el RGPD, no procedería la misma (Durán, 2016, págs. 760-761). A esto hay que añadir que, como el encargado debe informar en caso de tener una obligación legal que le obliga a tratar datos en contra de las instrucciones del responsable, este no deja de tener el control y podrá decidir si quiere seguir con el encargo o no.

(32)También se plantea la duda respecto a las personas sometidas a la autoridad de responsable y encargado que, como se ha indicado según el artículo 29 RGPD, y tal como se preveía en la Directiva 95/46/CE, también podían desviarse de su deber de seguir los dictados de estos si la legislación así lo disponía.

El RGPD incorpora un cuadro sancionador en caso de incumplimiento de sus preceptos, de forma que el sujeto obligado a cumplirlos será el potencial sancionado.

Así, se establece que las infracciones de las obligaciones del responsable y del encargado, a tenor de los artículos 8, 11, 25 a 39, 42 y 43, se sancionarán con multas de 10.000.000 € o, si es una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. También podrá ser sancionado el encargado mediante el tramo superior de multas de 20.000.000 € o de la cuantía equivalente al 4 % del volumen de negocio total anual global si es una empresa, cuando incumpla la regulación de las transferencias internacionales, las obligaciones que establezca la legislación nacional adoptada en virtud del capítulo IX del RGPD o el incumplimiento de resoluciones, limitaciones del tratamiento o suspensión de flujos de datos o no permitir el acceso a la autoridad de control (art. 83 RGPD).

En consecuencia, el encargado del tratamiento podrá ser sancionado por incumplir las obligaciones que tenga asignadas en el cuerpo del RGPD. Asimismo, en virtud de las reglas de atribución de responsabilidad que hemos visto entendemos que, cuando se convierta en responsable, será también sancionado por el incumplimiento de las obligaciones que como tal debiera haber cumplido.

Los interesados tienen derecho a presentar reclamaciones frente a las autoridades de control ante tratamientos de datos que consideren que infrinjan el RGPD. También se dispone que los interesados puedan interponer recursos judiciales contra los responsables o encargados cuando consideren que los derechos que les brinda el RGPD han sido vulnerados como consecuencia de un tratamiento de sus datos (art. 79.1 RGPD). En este caso, el órgano jurisdiccional ante el que debe interponerse el recurso será el de aquel Estado miembro en el que el responsable o el encargado tenga un establecimiento o también el

de aquel Estado miembro en el que el interesado tenga su residencia habitual, excepto si es una autoridad pública que actúe en ejercicio de poder público (art. 79.2 RGPD).

A ello hay que añadir que cualquier persona que haya sufrido daños y perjuicios materiales o inmateriales, como consecuencia de una infracción del RGPD, tendrá derecho a recibir del responsable o del encargado del tratamiento una indemnización por los daños y perjuicios sufridos (art. 82.1 RGPD). La diferencia más notable respecto a la Directiva 95/46/CE es, precisamente, la ampliación de la responsabilidad al encargado y la aclaración de que los daños a indemnizar son tanto los materiales como los inmateriales. Esta ampliación al encargado, sin embargo, en la legislación española ya existía (art. 19 LOPD). La infracción del RGPD, que puede acarrear el deber de indemnizar, también incluye la infracción de actos delegados y de ejecución y del derecho de los Estados miembros que especifique las normas del reglamento (Considerando 146 RGPD).

Mientras que el responsable implicado en la operación del tratamiento será responsable del daño causado si esta operación no cumple con el Reglamento, el encargado responderá por el daño causado por el tratamiento solo si no ha cumplido con las obligaciones que el Reglamento establece para este y por actuar fuera del ámbito o en contra de las instrucciones legales del responsable (art. 82.2 RGPD).

Tal como se establecía en la Directiva 95/46/CE, el responsable, y ahora el encargado también, podrán estar exentos de la responsabilidad si demuestran que no son responsables del hecho que ha causado los daños y perjuicios (art. 82.3 RGPD).

Si más de un responsable o encargado, que hubiera participado en la misma operación de tratamiento, debiera ser considerado responsable, de acuerdo con los criterios ya mencionados, debería responder por todo el perjuicio (art. 82.4 RGPD). Sin embargo, si se acumula en la misma causa, de conformidad con el derecho de los Estados miembros, la responsabilidad de responsables y encargados, la indemnización podrá prorratearse en función de esta responsabilidad de cada responsable o encargado, siempre que se garantice esta indemnización total y efectiva al interesado (Considerando 146 RGPD).

Si uno de los responsables o encargados se hace cargo del pago de este importe total, podría repetir contra los demás por la parte de la indemnización que correspondiera a las responsabilidades respectivas (art. 82.5 RGPD).

3. Los servicios de *cloud computing*

Al igual que sucedió con la energía eléctrica principios del siglo XX, cuando se pasó de disponer de generadores propios a consumir electricidad que proporcionaban proveedores en función de las necesidades del usuario, ha sucedido con la tecnología (Carr, 2005; Mell y Grance, 2011). Inicialmente, las empresas invertían en sistemas informáticos que se instalaban en su propia ubicación y que exigían de un mantenimiento. Con el aumento de velocidad de comunicación en internet y de la capacidad de almacenamiento de información, empresas que habían invertido en grandes centros de datos decidían convertirse en proveedores de servicios de alojamiento de información en estas instalaciones.

Referencias bibliográficas

N. Carr (2005). «The end of corporate computing». MIT Sloan Management Review.

P. Mell; T. Grance (2011, septiembre). *The NIST definition of cloud computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145*. NIST, US Department of Commerce.

Los proveedores de este tipo de servicios podían ser muy competitivos, ya que ubicaban sus centros de datos en lugares donde les era más económico la instalación de los mismos y utilizaban servicios de mantenimiento que podían hallarse también en otros países donde fueran más asequibles. Estos nuevos servicios se bautizaron como *cloud computing* (computación en la nube). Sus clientes disminuían los costes al evitar tener que adquirir y mantener sus sistemas informáticos.

3.1. Definición y modalidades

Para definir lo que es el *cloud computing* se suele acudir al concepto que estableció el National Institute of Standards and Technology (NIST). El *cloud computing* es un modelo de prestación de servicios tecnológicos que permite el acceso previa demanda, desde cualquier lugar, a través de la red, a un conjunto de recursos informáticos compartidos y configurables (como redes de comunicación, servidores, capacidad de almacenamiento, aplicaciones informáticos y servicios), que pueden ser rápidamente suministrados con un mínimo esfuerzo o mínima intervención del proveedor.

La denominación de *cloud computing*

La denominación de *cloud computing*, es decir, computación en la nube, deriva de la manera en la que se ilustra internet en los diagramas de arquitectura de sistemas informáticos, en los que se representa mediante una nube (Carr, 2005).

Las características esenciales de este servicio, según este documento, son: el autoaprovisionamiento previa solicitud (*on-demand self-service*); el acceso a través de una red (*broad network access*), que permite que desde cualquier dispositivo se pueda conectar; la puesta en común de recursos (*resource pooling*) que permite poner a disposición de los usuarios una multitud de recursos físicos y virtuales que se asignan de forma dinámica; la elasticidad (*rapid elasticity*), de forma que el suministro es automático y rápidamente escalable, según la demanda; servicio medido (*measured service*), de forma que se ajusta exactamente a las necesidades, ya que se puede monitorizar y medir exactamente el uso que se hace del mismo.

En este documento se diferencian tres tipos de modalidades de servicio de *cloud computing* y cuatro modelos de desarrollo de los mismos.

Las modalidades de servicios, que se distinguen, son el software como servicio, (*software as a service* o SaaS), en la que el proveedor de servicios de *cloud computing* proporciona servicios que permiten a los usuarios el uso de programas informáticos alojados en la infraestructura del proveedor.

La infraestructura como servicio (*infrastructure as a service* o IaaS), en la que el proveedor de servicios proporciona la infraestructura para que el usuario aloje las aplicaciones que quiera y pueda gestionarlas, pero sin que pueda gestionar la infraestructura del proveedor que incluirá las redes, servidores, sistemas operativos o almacenamiento.

Finalmente, la plataforma como servicio (*platform as a service* o PaaS), en la que el proveedor ofrece las herramientas para que el usuario pueda desarrollar sus aplicaciones. El usuario no tendrá control sobre la infraestructura del proveedor, aunque sí tendrá la posibilidad de gestionar los sistemas operativos, el almacenamiento, las aplicaciones y los componentes de comunicaciones. Se trata normalmente de una solución para empresas que necesitan desarrollar sus propias aplicaciones, o que son proveedores de servicios tecnológicos.

Según la modalidad de servicio de la que se trate, el control que tiene el cliente de la tecnología es mayor o menor, de forma que en la plataforma como servicio, el cliente tendrá el máximo control sobre la infraestructura, seguido de la infraestructura como servicio y, por último, estaría el software como servicio, respecto al que el cliente tendría la menor capacidad de control.

Respecto a los modelos de desarrollo de los servicios, se distingue si la nube es privada, pública, comunitaria o híbrida (*private cloud, community cloud, public cloud* o *hybrid cloud*, respectivamente). En la nube privada la infraestructura la utiliza una única organización y puede gestionarla ella misma, un tercero o ambos. La nube comunitaria la utiliza una multitud de usuarios de distintas organizaciones, que tienen algún interés en común, y puede pertenecer o ser gestionada por una o más organizaciones de esta comunidad, por un tercero o por una combinación de estos. En la nube pública puede utilizar los servicios el público, en general, y puede pertenecer la infraestructura a empresas u otros tipos de organización (como universidades o Administraciones públicas). La infraestructura en este caso estará en la ubicación del proveedor. La nube híbrida combinaría diversos de estos modelos (público, privado o comunitario).

La nube privada ofrecerá más garantías en cuanto a la seguridad y también en cuanto a cuestiones relacionadas con el cumplimiento legal, ya que podrá ser controlado por el cliente. Sin embargo, la nube privada conllevará mayores costes. La nube pública, por el contrario, implicará menor control por parte del cliente, pero conllevará un menor coste.

Si bien hay que tener presente esta definición de *cloud computing* porque nos ayuda a clasificar de alguna manera los servicios de este tipo, hay que tener presente que estamos frente a una tecnología cambiante que se une a otros desa-

rrollos tecnológicos que amplían sus posibilidades de negocio. Como ejemplo, baste citar la utilización de dispositivos portátiles o *smartphones* de gran capacidad, o la aparición de *apps* o la conocida como internet de las cosas o *internet of things*, que permite que objetos de todo tipo se conecten a internet y se pueda transmitir información a servicios de *cloud computing*. Los datos que se transmiten a raíz del uso de todos estos servicios o aparatos confluyen en internet en lo que se ha llamado *big data*, de forma que puede procesarse y analizar para obtener más información. Por ello, hay que evitar un análisis jurídico-estático y tener en cuenta los cambios tecnológicos para conocer cómo pueden afectar al derecho de protección de datos de las personas.

3.2. El proveedor de servicios de *cloud computing*, ¿encargado o responsable?

Con el fin de determinar la regulación aplicable, tal como hemos visto anteriormente, es necesario establecer el rol de los sujetos que participan en el servicio de *cloud computing*, cliente y proveedor de servicios. Para ello, acudiremos a las definiciones de responsable y encargado del tratamiento. Recordamos la definición de responsable contenida en el RGPD:

> ««Responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales; si el derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el derecho de la Unión o de los Estados miembros» (art. 4.7 RGPD).

3.2.1. Los elementos subjetivo y objetivo de las definiciones

El elemento subjetivo de la definición admite un número amplio de candidatos a ser responsable: «la persona física o jurídica, autoridad pública, servicio u otro organismo». Sin embargo, lo mismo sucedería si tomamos la definición de encargado que se refiere a «la persona física o jurídica, pública o privada, u órgano administrativo» (art. 5.1.i RLOPD).

El cliente del servicio puede ser un usuario individual, un consumidor, o puede ser una empresa o una Administración pública. El proveedor puede ser una única empresa o puede subcontratar a otras empresas y también puede ser una Administración pública. Por lo tanto, todos estos sujetos cumplirían con el elemento subjetivo de ambas definiciones.

No obstante, este tipo de servicios de *cloud computing* son habitualmente multicapa, de forma que hay diversos prestadores implicados en la prestación del mismo. Lo realmente complejo es desentrañar qué sujetos están detrás de estas capas, especialmente cuando el análisis lo debe realizar el cliente.

> Por ejemplo, un servicio de chat de soporte puede estar contratado a un tercero y, visualmente, aparecer totalmente integrado en el sitio web del servicio de *cloud computing*. El cliente tendrá la percepción de que el servicio se lo presta el proveedor con quien ha contratado, cuando en realidad es otro sujeto quien lo lleva a cabo o quien presta su

plataforma al proveedor principal. De hecho, la integración de *apps* de terceros es algo que promueven servicios, como las redes sociales, con el fin de crear contenido adicional para sus usuarios. En ese caso habrá que analizar cómo se realiza esta integración y, especialmente, si se proporciona acceso a los datos de los usuarios.

Y es que, aunque pudiéramos pensar en acudir al contrato de prestación de servicios para obtener esta información, lo normal es que en el mismo no aparezcan los proveedores subcontratados. De hecho, incluso al requerir la información al proveedor principal no es tan fácil obtenerla, ya que estos proveedores suelen ser empresas de gran tamaño en las que no todos los interlocutores conocen completamente los detalles del servicio que se proporciona o no tienen la conciencia de estar subcontratando un servicio que accede a datos personales.

En conclusión, al tratarse de servicios multicapa, uno de los aspectos más importantes para poder cumplir con la normativa, en los servicios de *cloud computing*, será conocer exactamente los detalles del servicio que se contrata, con el fin de realizar un análisis jurídico correcto.

Si seguimos desgranando los conceptos de responsable y encargado, podemos identificar el elemento objetivo, es decir, el objeto sobre el que actuarían estos sujetos y que sería «el tratamiento de datos», en ambos casos. Por tanto, deberíamos analizar si estamos ante un tratamiento de datos personales de acuerdo con el RGPD, es decir, si nos encontraríamos dentro del ámbito de aplicación material del RGPD.

Una de las cuestiones que se han planteado al respecto, en el ámbito de los servicios *cloud computing*, es la posibilidad de evitar la aplicación de la legislación de protección de datos con la utilización de técnicas de anonimización, cifrado y fragmentación. De esta forma, si los datos que se proporcionan al proveedor de *cloud computing* no le permiten identificar ni hacer identificables a las personas titulares, al menos respecto a este proveedor se tendría que considerar que no se aplicaría la normativa, porque no habría datos de carácter personal[33].

(33)Durán, 2016, págs. 615-616.

Fragmentación de datos

La fragmentación o dispersión de los datos es una técnica que se utiliza en los servicios de *cloud computing* que, sin aplicar el cifrado, pretende lograr un efecto similar. Consiste en fragmentar la información almacenada que se dispersa entre diferentes servidores. Si la dispersión se utiliza junto al cifrado se incrementa la seguridad (Cloud Security Alliance, 2011, pág. 52).

En este sentido, el RGPD introduce, en la parte de los considerandos, los criterios que había proporcionado el GA29 para valorar cuándo puede estimarse que una persona es identificable y, por tanto, entender que se tratan datos personales de la misma. Deben valorarse los medios, como la singularización, que puedan ser razonablemente utilizados por el mismo responsable o por cualquier otro individuo para identificar o distinguir directa o indirectamente

(34)Sentencia del TJUE de 19 de octubre de 2016, Patrick Breyer/BundesrepublikDeutschland, C-582/2014, EU:C:2016:779.

a dicha persona (Considerando 26 RGPD)[34]. Para establecer esta razonabilidad, se debe acudir a factores objetivos como los costes o el tiempo necesarios para realizar la identificación de la persona, así como la tecnología disponible no solo en el momento inicial del tratamiento, sino en todo el ciclo de vida del mismo.

El proceso de anonimización debería ser irreversible para el proveedor para que pudiera excluirse la aplicación de la legislación. Como indica la AEPD, el proceso debería producir la ruptura de la cadena de identificación de las personas y contemplar, durante todo el ciclo de vida del tratamiento, el riesgo de reidentificación. En el caso de que el proveedor aplicara técnicas de cifrado o de fragmentación, el GA29 las ha considerado equiparables al uso de seudónimos[35]. En este sentido, el RGPD contempla el uso de seudónimos como una medida de protección de los datos, pero se distingue claramente del proceso de anonimización, de forma que solo en este último caso se permitiría excluir la aplicación del RGPD (Considerandos 26, 28 y 29 RGPD)[36].

(35)Grupo de Trabajo Artículo 29 sobre Protección de Datos, págs. 17-24.

Reidentificación

La cadena de identificación se compone de microdatos o datos de identificación directa y de datos de identificación indirecta. Los microdatos permiten la identificación directa y los datos de identificación indirecta son datos cruzados de la misma o de diferentes fuentes que pueden permitir la reidentificación de las personas (Agencia Española de Protección de Datos, 2016, pág. 2).

(36)En el RGPD se define *seudonimización* como «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable» (art. 4.5 RGPD).

Otra cuestión problemática que se ha planteado en el marco de los servicios de *cloud computing* ha sido la relativa a las exclusiones del ámbito de aplicación de la normativa de protección de datos (Durán, 2016, págs. 616-617). Si el cliente de los servicios de *cloud computing* es una persona física, un consumidor final, puede ser que proporcione datos propios y se le califique como titular de estos datos que tratará el proveedor de servicios. También puede ser que proporcione datos de terceros (por ejemplo, de amigos, familiares o contactos) y debería analizarse si esta persona física también debe considerarse responsable, respecto a estos datos que proporciona al servicio de *cloud computing*. En ambos casos, habrá que ver si el proveedor de servicios actúa como responsable o no.

No obstante, como paso previo, es necesario valorar si estamos ante un tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas (art. 2.2.c RGPD). Como ejemplos de este tipo de actividades se mencionan, en el preámbulo del RGPD, «la correspondencia, la llevanza de un repertorio de direcciones o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades» (Considerando 18 RGPD).

En principio, en el caso de estas actividades no cabría aplicar el RGPD. No obstante, esta previsión, por el momento, hay que completarla con la jurisprudencia del TJUE interpretando la Directiva 95/46/CE, que estableció que

(37)Sentencia del TJUE, de 6 de noviembre de 2003, BodilLindqvist, C-101/01, EU:C:2003:596, apdo. 47.

no podrá incluirse en esta excepción un tratamiento de datos personales consistente en la difusión de estos datos por internet, de modo que resulten accesibles a un grupo indeterminado de personas[37].

De esta forma, en servicios de redes sociales, donde los usuarios son personas físicas que puede ser que publiquen datos personales de otras personas, si esta publicación se realiza de forma que estos datos sean accesibles a un grupo indeterminado de personas, no podrían aplicar la excepción y, por tanto, se les podrá considerar responsables de tratamiento, si se cumplen los otros elementos del concepto[38].

(38)Así, el GA29, en el marco de la Directiva 95/46/CE, consideraba que un usuario de una red social podrá ser calificado como responsable del tratamiento, sin que pudiera aplicarse esta excepción, cuando el usuario actuara, en nombre de una asociación o empresa o usara la plataforma con fines comerciales, políticos o benéficos. El GA29 también consideraba al usuario como un responsable cuando el usuario diera acceso a su perfil, más allá de un reducido grupo de contactos seleccionados (Grupo de Trabajo Artículo 29 sobre la Protección de Datos, pág. 6). Así lo indicaba también Troncoso, que destacaba que la inclusión de datos de otras personas en un perfil personal con un número elevado de contractos o abierto a todos los usuarios de la red social sin restricciones de acceso o al público en general a través de motores de búsqueda implicaba una publicación de datos donde no era posible identificar al cesionario y que suponía una cesión indiscriminada de datos (Troncoso, *Las redes sociales a la luz de la propuesta del reglamento general de protección de datos personales. Parte una*, pág. 72).

Sin embargo, el RGPD aclara que «se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas» (Considerando 18 RGPD). Es decir, los proveedores de servicios de *cloud computing* que permitan a las personas efectuar estas actividades no podrán aplicar esta exclusión en ningún caso, ya que los fines que persiguen con el tratamiento de datos personales de sus usuarios no encajarían en este ejercicio de actividades familiares y domésticas.

3.2.2. El poder de determinación de los fines y los medios del tratamiento

Una vez tenemos claro que estamos ante un tratamiento de datos incluido en el ámbito de aplicación del RGPD, nos quedaría determinar si los sujetos participantes en un servicio de *cloud computing* tienen la capacidad de determinar los fines y los medios del tratamiento de datos personales y, por tanto, deben ser considerados responsables.

Parece claro que el cliente, por regla general, determinará los fines, ya que es el que ha decidido contratar ese servicio y decidido entregar unos datos personales al proveedor. Si el proveedor decide utilizar los datos que el cliente le proporcione para una finalidad diferente a la prestación del servicio, también será considerado responsable.

En cambio, si lo que analizamos es quién determina los medios del tratamiento, ya no es tan fácil. Recordemos que, respecto a los medios, el GA29 distinguía dos tipos de elementos. Los elementos esenciales, que calificarían al sujeto de responsable, serían: los datos que se tratarán, las operaciones a realizar como la conservación y los terceros que tendrán acceso. Por otro lado, estarían los medios técnicos y organizativos, como el software o el hardware utilizados para el tratamiento, que no se considerarían, en principio, determinantes para calificar al responsable del tratamiento, sino que también podrían ser determinados por el encargado del tratamiento.

Si se mantiene esta interpretación realizada por el GA29, mientras el proveedor de servicios no determine los fines ni esos elementos esenciales, podrá ser considerado encargado del tratamiento si se cumple con los elementos de la definición de este sujeto.

> En este sentido, se puede citar el proyecto SLALOM, iniciativa financiada por la Comisión Europea a través del programa H2020, para desarrollar modelos contractuales para los servicios de *cloud computing*, que en el modelo de cláusulas contractuales elaborado limita al proveedor de servicios de *cloud computing*, que califica de encargado del tratamiento y que no podrá ir más allá de las instrucciones del cliente y determinar los fines y los medios esenciales del tratamiento (SLALOM Consortium, 2016, pág. 20).

Para poder saber si el cliente o el proveedor determinan los fines y los elementos esenciales de los medios del tratamiento, podremos acudir a la fuente de la que emana este poder de determinación. Puede originarse en la legislación, en el contrato suscrito por ambas partes o simplemente porque *de facto* el sujeto ha asumido ese poder. De hecho, como ya hemos indicado, sería la realidad la que debería primar en la calificación de los roles de los sujetos que traten los datos.

La legislación aplicable a los tratamientos nos dará, en muchos casos, la información que necesitamos para establecer el papel de los actores que participan en los mismos. Así, por ejemplo, las Administraciones públicas están sometidas a una intensa regulación que hace que no sea fácil que puedan traspasar el poder de determinación a un proveedor de servicios[39]. Otra cosa es que la realidad de los hechos nos muestre que sí existe este traspaso.

(39)Las Administraciones públicas tratan grandes volúmenes de datos de los ciudadanos y en ocasiones se trata de categorías especiales de datos. El Real decreto legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de contratos del sector público, dispone en su Disposición adicional 26.ª2 que, cuando «la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquel tendrá la consideración de encargado del tratamiento». Por lo tanto, en esta ley ya se califica al sujeto contratista como encargado del tratamiento de forma automática sin que quepa hacer ninguna valoración.

Sin embargo, como ya hemos comentado, el encargado del tratamiento podrá ir en contra de las instrucciones en virtud de la ley, lo que nos complicará la calificación del sujeto. Habrá que valorar, por lo tanto, el alcance de esta obligación legal del encargado para determinar si también pudiera suponer el origen del poder de determinación que sí deba convertirlo en responsable.

Otro elemento que nos ayudará en el análisis de la fuente de la que emana la capacidad de determinación del responsable son las condiciones contractuales. El primer indicio será si se trata de unas condiciones pactadas *ad hoc* o unas condiciones generales. En el primer caso, obviamente, de entrada habrá un mayor equilibrio entre las partes que habrán podido negociar las cláusulas. En el segundo caso, existirá un desequilibrio en beneficio de quien las ha impuesto, el proveedor.

En cualquier caso, pese a estos indicios, habrá que analizar el contrato para establecer a qué sujeto otorga el poder de determinar los fines y los elementos esenciales de los medios. Y es que, desde el año 2012, en el que se desarrollaron especialmente estos servicios de *cloud computing* y en el que se sitúan la mayoría de documentos de análisis jurídico de este fenómeno, se ha trabajado, tanto en el ámbito de las instituciones, como en el de los mismos proveedores, para intentar mejorar ese marco contractual.

En este sentido, se pueden señalar iniciativas de los proveedores como Amazon, que permite al cliente seleccionar la zona donde quiere que se ubiquen sus datos de manera que pueda ser en la región de la UE (Amazon Web Services, 2016, págs. 6-8).

Estos trabajos, en el ámbito de las instituciones, no solo han perseguido la mejora en la protección de datos, sino que también se han realizado para incentivar la utilización del *cloud computing* como motor de la economía europea. En esta línea, la Comisión Europea creó un grupo de expertos que ha trabajado en la elaboración de contratos tipo para estos servicios y que ha tenido en cuenta los aspectos relativos a la protección de datos[40].

(40)La promoción del uso del *cloud computing* estaba en uno de los pilares de la Agenda digital para desarrollar el mercado único digital. Entre las acciones concretas que se establecieron para promover ese uso, estuvo la de elaborar unas «condiciones contractuales seguras y justas» (Comisión Europea, 2012, págs. 13-15).

No solo habrá que analizar las condiciones contractuales, sino que habrá que acudir a la realidad de los hechos. ¿Cómo se puede verificar quién ostenta realmente el control, pese a lo que establezca el contrato? Podrá acudirse a toda la información sobre el servicio, que podrá hallarse en la plataforma o en los manuales que se proporcionen al cliente, los apartados de ayuda o la

(41)Article 29 Data Protection Working Party, 2015, págs. 7-8 e International Working Group on Data Protection in Telecommunications, 2012, págs. 2-3).

información comercial. En muchos casos, será en esta información donde hallaremos realmente la respuesta a quién asume el control sobre fines y medios. Como han señalado las autoridades de control, los riesgos que conlleva el uso de estos servicios para la protección de datos se pueden agrupar en la falta de información y de control sobre los datos[41]. Sin duda, son dos aspectos que van unidos, de forma que si el servicio es opaco para el cliente, eso implicará forzosamente que no tenga el control.

Si el cliente no conoce las subcontrataciones que realiza el proveedor o ignora que el proveedor recoge ciertos datos de los empleados del cliente, al utilizar el servicio o desconoce el tipo de operaciones a las que somete los datos o el lugar donde se ubican los datos, no podrá ejercer su capacidad de determinación. Por ello, la transparencia en la forma en la que el proveedor desarrollará el servicio será primordial, como paso preliminar para poder establecer si puede existir esa capacidad de determinación. En definitiva, tras verificar si existe esta información, deberá analizarse esta para concluir si la capacidad de determinación de fines y medios reside en el cliente o en el proveedor.

Sin embargo, la postura de las autoridades de protección de datos ha sido, principalmente, de simplificación, de forma que *a priori* se califica al cliente como responsable y al proveedor de servicios de *cloud computing* como encargado del tratamiento. La AEPD y el GA29 se decantaron por esta opción[42]. De esta forma, las autoridades incidieron en la responsabilidad del cliente, de su capacidad de elección del servicio[43].

(42)La AEPD, en los documentos que ha emitido para dar las pautas sobre el tema del *cloud computing*, señala claramente a los clientes como responsables y a los proveedores como encargados del tratamiento (Agencia Española de Protección de Datos, 2013, págs. 13-14; Agencia Española de Protección de Datos, 2013). El GA29 ha dictaminado que el hecho de que el contrato lo elabore el proveedor del servicio y no el responsable del tratamiento no es, por sí mismo, base suficiente para concluir que el proveedor del servicio deba considerarse el responsable del tratamiento, en la medida en que el responsable ha aceptado libremente las condiciones contractuales y, por lo tanto, la plena responsabilidad sobre estas. No se acepta que el desequilibrio en cuanto al poder contractual entre un pequeño responsable y un gran proveedor de servicios debiera considerarse una justificación para que el primero acepte unas condiciones que no se ajusten a la legislación de protección de datos (Grupo de Trabajo Artículo 29, 2010, pág. 29; Grupo de Trabajo Artículo 29 sobre Protección de Datos, pág. 10).

(43)En los supuestos normales de servicios de *cloud computing* donde un proveedor celebre contratos con sus clientes y les preste estos servicios mediante subcontratación de otras empresas, Rubí señala que no cabe duda de que este proveedor tiene una importante capacidad para tomar decisiones sobre estos servicios. Puede seleccionar a sus subcontratados y optar por el lugar donde se producirá el tratamiento o delimitar las medidas de seguridad. El autor, sin embargo, considera que esta capacidad de decisión no excluye que los clientes sigan ostentando esta condición de responsables; por tanto, estima que, como punto de partida, el prestador de servicio debe considerarse encargado del tratamiento (Rubí, 2012, págs. 93-94). Porcedda, en cambio, plantea si es necesario considerar al proveedor de servicios de *cloud computing* como un responsable y no un encargado del tratamiento (Porcedda, 2012, pág. 228).

Algunas autoridades matizaron esta calificación, como la autoridad de control francesa, que consideró, de entrada, que el proveedor podía ser calificado de responsable conjunto en estas situaciones en las que *de facto* el cliente no tenía capacidad de decidir. La autoridad francesa, la CNIL, consideró que, en este

tipo de servicios de *cloud computing*, sobre todo en los PaaS y SaaS públicos, quedaba patente que los clientes no podían realmente decidir ni dar instrucciones que garantizaran la efectividad de las garantías de seguridad y confidencialidad, que debían aportar los proveedores.

Por ello, el proveedor podía ser considerado *a priori* como responsable conjuntamente con el cliente, en virtud de la definición de responsable del tratamiento, ya que participaría en la determinación de los fines y los medios de los tratamientos. Incluso la CNIL sugería un reparto de responsabilidades formal entre ambos sujetos, de manera que, por ejemplo, la notificación de ficheros, la autoridad recomendaba que la llevara a cabo el cliente, así como el deber de informar a los interesados. En cambio, en cuanto a la obligación de cumplir con las medidas de seguridad y confidencialidad, así como la de atender el ejercicio de derechos de los interesados, la autoridad recomendaba que la repartieran entre ambos sujetos (CNIL, 2012, págs. 5-6).

Asimismo, el Supervisor Europeo de Protección de Datos también indicó que la complejidad técnica de este tipo de servicios podía implicar que el cliente no fuera el único en determinar los fines y los medios del tratamiento (European Data Protection Supervisor, 2012, pág. 12). El Supervisor indicó que la determinación de los elementos esenciales de los medios no era siempre una prerrogativa del cliente, ya que el proveedor habitualmente diseña, opera y mantiene la infraestructura tecnológica, que puede incluir desde servicios esenciales de hardware y software (en el IaaS), la plataforma (en el PaaS) o las aplicaciones (SaaS). Como indicaba el Supervisor, en los servicios de IaaS el cliente podría tener cierta capacidad de influencia en las condiciones del servicio, pero en el SaaS resultaría claro que no tiene capacidad de control sobre los medios del tratamiento y debería ser calificado el proveedor como corresponsable. Por tanto, el Supervisor consideró que, en este escenario, reflejaría mejor la verdadera relación de poderes de cliente y proveedor, respecto al tratamiento, el supuesto de corresponsabilidad (European Data Protection Supervisor, 2012, pág. 13).

Referencia bibliográfica

European Data Protection Supervisor (2012). *Opinion of the European Data Protection Supervisor on the Commission's Communication on «Unleashing the potential of Cloud Computing in Europe»*.

Hay que añadir que, durante la elaboración del RGPD, se abordó esta cuestión. La presidencia griega del Consejo de la UE insistió en que el desequilibrio que puede producirse en los servicios de *cloud computing*, por ser el proveedor una empresa de mayor envergadura que la del cliente, no puede implicar que el cliente deje de tener responsabilidad respecto al cumplimiento de la normativa que debe reflejarse en las condiciones contractuales suscritas (Council of EU, 2014, págs. 7-8) y (Council of EU, 2014). Por eso, lo que sugería la presidencia, como solución a este problema, era la adopción de modelos de contratos que podrían utilizarse entre el cliente responsable y el proveedor encargado del tratamiento, al igual que se hace en las transferencias internacionales. De esta forma, así se aseguraría que el contrato cumpliera efectivamente con lo establecido en la normativa de protección de datos. Puyol resalta la impor-

Referencias bibliográficas

Council of EU (2014). *Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data*. Bruselas.

J. Puyol (2013). *Algunas consideraciones sobre cloud computing, Premio protección de datos personales de investigación 2012*. Madrid: Agencia Estatal BOE.

tancia del contrato suscrito en el ámbito del *cloud computing* y considera que la determinación de los niveles de responsabilidad es una asignatura pendiente en el desarrollo del *cloud computing* (Puyol, 2013, págs. 60, 94-95).

En este sentido, cabe señalar los trabajos ya mencionados, que pretenden mejorar las condiciones contractuales, en el entorno de servicios de *cloud computing*. En el marco de estos trabajos también se planteó, a raíz de la postura de la autoridad francesa de protección de datos, que pudiera considerarse la posibilidad de establecer varios modelos de cláusulas contractuales, de forma que se pudiera optar entre considerar al proveedor encargado del tratamiento o responsable conjunto[44].

(44)(Commission Expert Group on Cloud Computing Contracts, 2014). Sin embargo, en el proyecto SLALOM ya mencionado, en el modelo de cláusulas contractuales elaborado se ha partido de la interpretación de que el proveedor es el encargado del tratamiento (SLALOM Consortium, 2016, pág. 20).

3.3. ¿Hasta qué punto el RGPD proporciona una respuesta a los servicios de *cloud*?

Como ya se ha indicado, el RGPD pretendía responder a las necesidades que el desarrollo tecnológico había planteado, pero nos preguntamos si realmente da una respuesta a los retos que han supuesto los servicios de *cloud computing*.

En primer lugar, en línea con el análisis efectuado sobre la calificación del proveedor de servicios como encargado o responsable del tratamiento, lo cierto es que habrá que esperar a la interpretación que realicen las autoridades de control ya que, como hemos visto, no tenían una postura unánime. En el caso de que se optara, en algún caso, por entender que el proveedor puede ser calificado como responsable, se podría acudir a una de las novedades que ha introducido el RGPD: la regulación de la corresponsabilidad.

Y es que el RGPD resalta la necesidad de una atribución clara de responsabilidades entre los participantes en el tratamiento de datos con el fin de asegurar la protección de los interesados, la supervisión de las autoridades y la responsabilidad de estos participantes (Considerando 79 RGPD). En consonancia con este objetivo, la regulación de la corresponsabilidad incide en la determinación de las responsabilidades respectivas de los corresponsables en el cumplimiento de las obligaciones del RGPD que debe realizarse de mutuo acuerdo y de forma transparente (art. 26.1 RGPD).

Sin embargo, pese al avance que supone la introducción de esta obligación de acuerdo entre los corresponsables, se nos antoja difícil que en el entorno de los servicios de *cloud computing* se pueda plantear en todos los casos este tipo de acuerdos. Hay que tener en cuenta, como se ha comentado anteriormen-

te, el carácter multicapa de estos servicios en los que puede ser que los corresponsables actúen de forma automática sin entrar en ninguna negociación ni acuerdo (Durán, 2016, págs. 762-763).

Otra cuestión que había sido problemática en los servicios de *cloud computing* era la aplicación de la normativa de protección de datos, no ya solo como se ha comentado respecto al ámbito subjetivo y objetivo, sino también al territorial. Y es que el hecho de que las autoridades tendieran a calificar al proveedor como encargado también fue provocado por la necesidad de proteger los datos de los nacionales frente a un proveedor que se ubicara en el extranjero. Si este proveedor pudiera calificarse como responsable con la anterior legislación se hacía más difícil aplicar la normativa europea de protección de datos al mismo. En cambio, si el proveedor se consideraba encargado facilitaba que se sometiera a esta legislación.

El RGPD, para responder a esta necesidad (que en parte se había solventado con la sentencia del TJUE en el asunto Google[45]), amplía el ámbito de aplicación territorial que incluye tanto a responsables como encargados que puedan dirigir sus servicios a los interesados en la UE o que puedan controlar el comportamiento de los mismos en la UE (art. 3.2 RGPD).

(45)Sentencia del TJUE de 13 de mayo de 2014, Google Spain, S. L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González, C-131/2012, EU:C:2014:317.

Si el proveedor de servicios de *cloud computing* es considerado encargado del tratamiento, ya hemos visto el contenido que debería tener el contrato con el cliente responsable. Con el fin de poder luchar contra el desequilibrio contractual que puede existir, sin duda es positiva la posibilidad de acudir a contratos tipo tal como se establece en el RGPD.

En este sentido, una de las cuestiones que también había suscitado problemas ante el desequilibrio contractual existente ante grandes prestadores de servicios era que el cliente tuviera que imponer las medidas de seguridad que establecía la legislación española. En este aspecto se logra una mayor flexibilidad, ya que con el RGPD, como hemos visto, no se incluye un catálogo concreto de medidas de seguridad, sino que se adopta un enfoque de riesgo, por lo que puede acudirse a estándares reconocidos internacionalmente[46] (Agencia Española de Protección de Datos, 2013, pág. 16). También se permite la posibilidad de acudir a códigos de conducta o mecanismos de certificación que demuestren el cumplimiento de los requisitos sobre seguridad.

(46)De hecho, esto es lo que la AEPD había aceptado mediante una modulación de la regulación en el ámbito de los servicios *cloud computing*. Así, la AEPD había adoptado un enfoque funcional respecto a las medidas de seguridad, de forma que aceptaba como garantía de que el proveedor cumplía con las medidas de seguridad una certificación adecuada o que un tercero auditara al proveedor, siempre que se conociera la entidad auditora y los estándares aplicados.

El RGPD permite la subcontratación, que exigirá que se cumplan los requisitos previstos. Otro aspecto importante en este entorno es la existencia de transferencias internacionales que pueden producirse a raíz de estas subcontrataciones. Esto obligará al proveedor a ser transparente, lo que ya en nuestra legislación se producía y que había dado lugar a que la AEPD propusiera algunas soluciones que hicieran factible esta información de los subcontratados mediante la página web del proveedor encargado del tratamiento (Agencia Española de Protección de Datos, 2013, pág. 14). Entendemos que esta fórmula de publicación en una página web podría seguir utilizándose.

Referencia bibliográfica

Agencia Española de Protección de Datos (2013). *Guía para clientes que contraten servicios de cloud computing*.

Si bien se establece el nuevo derecho a la portabilidad para los interesados, no se ha incluido en el RGPD que el encargado del tratamiento, proveedor de servicios de *cloud computing*, transfiera los datos del cliente directamente a un nuevo proveedor de servicios[47] (Agencia Española de Protección de Datos, 2013, pág. 7).

(47)Algo que de nuevo había indicado la AEPD que debía realizarse, lo que estaba en consonancia con el artículo 22.1 RLOPD, que establecía que, al finalizar la prestación de servicios, los datos debían ser destruidos o devueltos al responsable o al encargado que este hubiese designado.

En conclusión, si bien en algunos aspectos se ha podido dar respuesta a algunas de las problemáticas existentes en este sector, principalmente con fórmulas más flexibles como la autorregulación, en otras se mantiene una rigidez que dificultará su adaptación a este entorno, como en el caso de la corresponsabilidad.

4. Autorregulación

En línea con el nuevo enfoque que sigue el RGPD relativo a la responsabilidad proactiva, se han impulsado en el texto los mecanismos de autorregulación. Así, al lado de los ya conocidos códigos de conducta, se añaden las certificaciones. Ambas fórmulas pretenden incidir en la prevención y se contemplan como una vía para hacer más flexible la adaptación al desarrollo tecnológico. Estas fórmulas servirán a los sujetos obligados a demostrar su compromiso con el cumplimiento.

4.1. Códigos de conducta

Los códigos de conducta, como hemos indicado, no son una novedad ya que se establecían en la Directiva 95/46/CE y en nuestra legislación[48]. Los códigos tienen como objetivo incentivar el cumplimiento por parte de los sujetos obligados, de forma que contribuyan a la correcta aplicación del RGPD, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pymes.

[48]En la LOPD se denominaban códigos tipo (art. 32 LOPD) y su regulación se desarrolló ampliamente en los artículos 71 y siguientes del RLOPD.

El RGPD establece la posibilidad de que asociaciones y organismos que representen a categorías de responsables o encargados del tratamiento elaboren, modifiquen o amplíen códigos de conducta y que puedan presentarlos ante la autoridad de control, con el fin de que emita un dictamen acerca de la conformidad con el Reglamento y lo apruebe si considera suficientes las garantías adecuadas que ofrece (art. 40.2 y 5 RGPD). En caso de que la autoridad de control apruebe el código, la modificación o ampliación, lo registrará y lo publicará.

Si el código proyectado se refiriera a actividades de tratamiento en varios Estados miembros, la autoridad de control se lo presentará al Comité Europeo de Protección de Datos (organismo que sustituye al GA29). Este Comité dictaminará si el proyecto es conforme con el RGPD o si ofrece garantías adecuadas. Si el dictamen es positivo, el Comité lo presentará a la Comisión, que podrá decidir que este código, la modificación o ampliación tengan validez dentro de la UE. La Directiva 95/46/CE ya contemplaba que los códigos de conducta pudieran tener este alcance europeo y que, para ello, debían ser sometidos al GA29. Sin embargo, la complejidad que supone respetar normativas nacionales en ocasiones divergentes y el riguroso proceso de aprobación, que exigía un valor añadido en el cumplimiento han supuesto un escaso éxito de los códigos de conducta europeos[49] (Article 29 Data Protection Working Party, 2015).

[49]Así, por ejemplo el GA29 no aprobó el código de conducta presentado en 2015 por Cloud Select Industry Group (C-SIG) sobre el *cloud computing*.

Referencia bibliográfica

Article 29 Data Protection Working Party (2017). *Guidelines on Data Protection Officers (DPOs)*.

Sin perjuicio de las funciones de las autoridades de control, se ha establecido que el código de conducta debe incluir mecanismos que permitan su supervisión por un organismo específico que será acreditado por la autoridad de control competente (art. 41.1 RGPD). Este organismo podrá adoptar medidas en caso de infracción del código por un responsable o encargado, incluyendo la suspensión o exclusión, de lo que informará a la autoridad de control (art. 41.4 RGPD). Hay que recalcar que, además, este organismo será susceptible de ser sancionado en caso de incumplir sus obligaciones (art. 83.4.c RGPD).

4.2. La certificación

Como hemos indicado, el RGPD incluye un nuevo mecanismo: los mecanismos de certificación. Y es que el principio de responsabilidad proactiva enlaza con el desarrollo de sistemas de certificación, de forma que parece una evolución natural (Durán, 2016, pág. 737). En un primer momento, el responsable del tratamiento debe instaurar las medidas adecuadas para cumplir con la normativa. Posteriormente, el responsable del tratamiento podría acudir a un sistema de certificación que evaluase que efectivamente aplica estas medidas. De esta forma, el responsable podría obtener un certificado o sello que hiciera visible su esfuerzo en asegurar un correcto cumplimiento. Por tanto, el responsable obtendría así una forma de diferenciarse en el mercado. Además, este sistema de certificación se puede utilizar para facilitar la supervisión que las autoridades de protección de datos puedan llevar a cabo.

Tanto los códigos de conducta como los mecanismos de certificación incluidos en el RGPD constituyen el resultado de la tendencia en la utilización de fórmulas de autorregulación regulada. Esto implica la autorregulación por parte de los responsables, aunque sometida a una regulación y a una supervisión por parte de las autoridades de control o los organismos acreditados con este fin. De hecho, ya existen certificaciones incluso de alcance europeo que se utilizan para revisar el respeto de la legislación de protección de datos.

> En este sentido cabe citar, como ejemplo, la certificación EuroPriSe (European Privacy Seal) que impulsó en un inicio la autoridad de control del Land alemán de Schleswig-Holstein. Este proyecto de certificación de productos de software y servicios web revisa si los mismos son compatibles con la legislación europea de protección de datos. El proyecto fue financiado por la Comisión Europea y apoyado por algunas autoridades de control, entre la que figuró la extinta Agencia de Protección de Datos de la Comunidad de Madrid, de la mano de Antonio Troncoso, que fue director de la misma. Troncoso entendía que la opción de este sistema, en el que los que realizan la evaluación de los productos o servicios son expertos acreditados, es mejor que optar por que fueran las mismas autoridades de control las que llevaran a cabo la evaluación (Troncoso, 2010, págs. 257-258).

La adhesión a códigos de conducta o los mecanismos de certificación podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones del responsable (art. 24.3 RGPD).

La certificación podrá expedirla los organismos de certificación o la autoridad de control competente sobre la base de los criterios aprobados por dicha autoridad o por el Comité Europeo de Protección de Datos (art. 42.5 RGPD). Si los criterios los aprueba este Comité, esto dará lugar a una certificación común (se entiende que de alcance europeo): el Sello Europeo de Protección de Datos, aunque se limita el período de validez de este sello a tres años, pudiendo ser renovado o retirado si se dejan de cumplir los requisitos. Los órganos de certificación se hallan regulados en el artículo 43 RGPD y pueden ser acreditados por una autoridad de control o por el organismo nacional de acreditación, o por ambos. Al igual que los organismos de supervisión de los códigos de conducta, también estos órganos de certificación podrán ser sancionados si incumplen sus obligaciones (art. 83.4.b RGPD).

Un aspecto novedoso es el referido a la posibilidad de que responsables o encargados no sujetos al reglamento puedan adherirse a los códigos de conducta o a los mecanismos de certificación, con el fin de que pudieran servir como garantías para poder realizar transferencias internacionales de datos (arts. 40.3 y 42.2 RGPD).

Se han establecido multas administrativas en caso de infracción de las obligaciones establecidas en los artículos 42 y 43 RGPD para los responsables y encargados, preceptos que contienen la regulación de los mecanismos de certificación. Asimismo, se ha acogido que la utilización de estos instrumentos, tanto códigos de conducta como mecanismos de certificación, sea un factor que ayude a reducir las sanciones administrativas que pudieran imponerse al responsable o encargado en caso de que se hubieran adherido a los mismos (art. 83.2.j) RGPD). Es esencial que se otorgue algún incentivo cuando se usen estos instrumentos, ya que supone una inversión en tiempo y recursos por parte de los responsables (Durán, 2016, pág. 740). Sin embargo, hay que tener en cuenta que, pese a estas ventajas establecidas ante el uso de la certificación, también se precisa que ello no puede limitar la responsabilidad de responsables o encargados en cuanto al cumplimiento del RGPD (arts. 42.4 RGPD).

Resumen

Con este módulo se ha querido ofrecer una panorámica de la regulación de las transmisiones de datos. Para ello, se ha tenido en cuenta la encrucijada en la que está la legislación de protección de datos. La regulación específica de las cesiones de datos en la LOPD quedará superada por la aplicación del RGPD, que si bien incluye preceptos que hacen referencia a esta operación, no establece, como la LOPD, una regulación específica y completa. Sin duda, hay que centrarse en la nueva norma que desplazará las normativas nacionales y que tiene como antecedente la Directiva 95/46/CE, adquiriendo gran importancia las interpretaciones que de la misma han realizado las autoridades en el marco del GA29, así como las sentencias del TJUE.

Si era importante, y quizás una de las cuestiones más complejas en materia de protección de datos, el hecho de diferenciar entre responsable del tratamiento y encargado del tratamiento, con el RGPD ello aún es más trascendente. Y es que en esta norma el encargado adquiere una mayor relevancia de la que tenía en la Directiva 95/46/CE. Esto se refleja en el establecimiento de una serie de obligaciones y de su responsabilidad. Al contrario de lo que sucedía con la cesión, en la regulación que proporciona el RGPD del encargado del tratamiento hemos visto una gran semejanza con la regulación contenida en el artículo 12 de la LOPD y en los artículos 20 y siguientes del RLOPD.

Hemos ilustrado las dificultades acerca de la determinación de si un sujeto puede ser calificado de responsable o de encargado con los servicios de *cloud computing*, paradigma del desarrollo tecnológico al que el RGPD pretende adaptarse. El RGPD aborda algunas de las cuestiones que, en materia de protección de datos, se han ido planteando respecto a este tipo de servicios, como la aplicación a los proveedores que se hallaban fuera de la UE. Sin embargo, respecto a la calificación del proveedor de *cloud computing* como responsable o encargado, habrá que ver la interpretación que realicen las autoridades. Si dicho proveedor fuera calificado como responsable, se incluye en el RGPD una nueva regulación sobre la corresponsabilidad que sería aplicable al proveedor y a su cliente.

Por último, se ha hecho mención al impulso que el RGPD realiza, en coherencia con el enfoque de responsabilidad proactiva, a los mecanismos de autorregulación. Los códigos de conducta y las certificaciones serán las herramientas que tanto los responsables como los encargados podrán utilizar para acreditar su cumplimiento.

Bibliografía

Agencia Española de Protección de Datos (2013). *Guía para clientes que contraten servicios de cloud computing*.

Agencia Española de Protección de Datos (2013). *Orientaciones para prestadores de servicios de cloud computing*.

Agencia Española de Protección de Datos, Autoritat Catalana de Protecció de Dades, Agencia Vasca de Protección de Datos. *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*.

Amazon Web Services (2016). *Whitepaper on EU Data Protection*. [Fecha de consulta: 19 de junio de 2017].

<https://d0.awsstatic.com/
whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper_EN.pdf>

Article 29 Data Protection Working Party (2014). *Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218*.

Article 29 Data Protection Working Party (2015). *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing 2588/15/EN WP 232*.

Article 29 Data Protection Working Party (2017). *Guidelines on Data Protection Officers (DPOs)*.

Carr, N. (2005). «The end of corporate computing». *MIT Sloan Management Review*.

CNIL (2012). *Recommandations pour les entreprises qui envisagent de souscrire à des services de cloud computing*.

Comisión Europea (2012). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Liberar el potencial de la computación en nube en Europa, COM(2012) 529 final*. Bruselas.

Commission Expert Group on Cloud Computing Contracts (2014). *Liability for non-compliance with data protection obligations, rough draft presented by M-CH. ROQUES-BONET, L. NETO GALVAO*.

Council of EU (2014). *Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX) on specific issues of Chapters I-IV of the General Data Protection Regulation-certain aspects of the relationship between controllers and processors*. Bruselas.

Council of EU (2014). *Note from Presidency to Working Group on Information Exchange and Data Protection (DAPIX). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data*. Bruselas.

Durán, B. (2016). *La figura del responsable en el derecho a la protección de datos*. Madrid: Wolters Kluwer.

European Data Protection Supervisor (2012). *Opinion of the European Data Protection Supervisor on the Commission's Communication on «Unleashing the potential of Cloud Computing in Europe»*.

Grupo de Trabajo Artículo 29 (2010). *Dictamen 1/2010 sobre los conceptos de responsable del tratamiento y encargado del tratamiento, 00264/10/ES WP 169*.

Grupo de trabajo Artículo 29. sobre Protección de Datos . *Dictamen 5/2012 sobre la computación en nube, 01037/12/ES WP 196, 1.7.2012*.

Heredero, M. (1997). *La Directiva comunitaria de protección de los datos de carácter personal (Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales*. Cizur Menor: Aranzadi.

International Working Group on Data Protection in Telecommunications (2012). *Working paper on cloud computing-Privacy and data protection issues, «Sopot Memorandum»*. Sopot, Polonia.

Mell, P.; Grance, T. (2011, septiembre). *The NIST definition of cloud computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145*. NIST, US Department of Commerce.

Messía de la Cerda, J. (2003). *La cesión o comunicación de datos de carácter personal*. Cizur Menor: Aranzadi.

Porcedda, M. (2012). «Law enforcement in the clouds: is the EU data protection legal framework up to the task?». En: S. Gutwirth; R. Leenes; P. de Hert; Y. Poullet. *European Data Protection: in good health?* (págs. 203-232). Países Bajos: Springer.

Puyol, J. (2013). *Algunas consideraciones sobre cloud computing, Premio protección de datos personales de investigación 2012*. Madrid: Agencia Estatal BOE.

Rubí, J. (2012). «El proveedor de cloud como encargado del tratamiento». En: R. Martínez. *Derecho y cloud computing*. Cizur Menor: Aranzadi.

SLALOM Consortium. (2016). *Model contract for Cloud computing*.

Troncoso, A. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch.

Troncoso, A. (s. f.). «Las redes sociales a la luz de la propuesta del reglamento general de protección de datos personales. Parte una». *IDP. Revista de Internet, Derecho y Política* (núm. 15).