Sujetos que intervienen en el tratamiento

PID_00246873

Antoni Roig

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Antoni Roig

Índice

1. Sujetos públicos y privados

El Reglamento general de protección de datos (en adelante, RGPD) garantiza el derecho a la protección de los datos personales de las personas físicas. Este cometido no podrá impedir la libre circulación de datos personales en la Unión Europea. Será de aplicación a los datos personales que obren en poder de las instituciones, órganos y organismos de la Unión Europea el Reglamento 45/2001[1], que deberá, en todo caso, interpretarse de acuerdo con el RGPD.

La nueva LOPD

Pese a ser de directa aplicación, el RGPD será complementado por una nueva LOPD, cuyo anteproyecto (en adelante, APLOPD) ya se encuentra disponible, aunque no ha sido todavía aprobada la futura LOPD cuando se remite la última versión de este apartado, a finales de julio del 2017. El APLOPD indica que su función es clarificar el RGPD, eliminar situaciones de incertidumbre debidas a la anterior LOPD y complementar el RGPD.

(1)Reglamento (CE) 45/2001, de 18 de diciembre, de protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. El 10 de enero del 2017, la Comisión Europea propuso un nuevo Reglamento que derogará al Reglamento 45/2001 y la Decisión 1247/2002/CE, con el fin de adaptarlos al RGPD.

Lecturas recomendadas

Sobre el derecho a la protección de los datos personales de las personas físicas, podéis leer:

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril del 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.

R. Martínez (2012). «El complejo encaje normativo de la propuesta de Reglamento general de protección de datos de la Unión Europea». *Actualidad Jurídica Aranzadi* (núm. 839, pág. 3).

J. M. Hernández (2013). *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*. Cizur Menor: Aranzadi.

A. Rallo; R. García (ed.) (2015). *Hacia un nuevo derecho europeo de protección de datos* (*Towards a new European data protection regime*) (págs. 29-81). Valencia: Tirant lo Blanch.

A. Troncoso (2012). «Hacia un nuevo marco jurídico europeo de protección de datos personales». *Revista Española de Derecho europeo* (núm. 43, págs. 25-184). Cizur Menor: Aranzadi.

Antes de estudiar los sujetos públicos y privados que intervienen en el tratamiento de los datos personales, definiremos lo que se entiende por tratamiento:

«Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción» (artículo 4 RGPD, definiciones).

Pues bien, los sujetos que intervienen en el tratamiento son el interesado, el responsable del tratamiento, el encargado, el destinatario y el tercero. Veremos en el siguiente apartado al responsable y al encargado del tratamiento. Aquí describiremos lo que entendemos por interesado, destinatario y tercero.

El interesado es una persona física identificada o identificable, cuya identidad pueda determinarse, de manera directa o indirecta, mediante un identificador: un nombre, un número, datos de localización, un elemento físico, fisiológico, genético, psíquico, económico, cultural o social de una persona (art. 4 RGPD, definiciones, «datos personales»). Por consiguiente, el interesado no puede ser una persona jurídica, a diferencia de lo previsto en la propuesta de reglamento de la Unión sobre privacidad y comunicaciones electrónicas. electrónicas, de 10 de enero de 2017 (Reglamento ePrivacy), que sustituirá a la Directiva 2002/58 de ePrivacy.

Nota

Por consiguiente, el interesado no puede ser una persona jurídica, a diferencia de lo previsto en la propuesta de reglamento de la Unión sobre privacidad y comunicaciones electrónicas de 10 de enero de 2017 (Reglamento ePrivacy), que sustituirá la Directiva 2002/58 de ePrivacy.

Por su parte, el destinatario es una persona física o jurídica, servicio u otro organismo al que se comuniquen datos personales. Puede ser un tercero o no. Si los datos se comunican a una autoridad pública que lleva a cabo una investigación de acuerdo con el Derecho europeo, no se considerará a la misma como destinataria, y se regirá por las normas de protección de datos aplicables a los fines concretos del tratamiento (art. 4 RGPD, «destinatario»).

Finalmente, el tercero será una persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable, del encargado y de las personas autorizadas por estos últimos (art. 4 RGPD, «tercero»). La clave es no ser parte de una entidad o acuerdo. Así, personas que trabajan para otra organización, incluso si pertenece a un mismo grupo o sociedad, serán, en general, terceros. En cambio, las filiales de un banco, dado que se encuentran bajo la autoridad directa de la sede central, no serán consideradas como terceros. Por tanto, un tercero que recibe datos personales puede acabar siendo un nuevo responsable si lleva a cabo un tratamiento con los mismos que se rija por el RGPD.

2. El responsable y el encargado del tratamiento

2.1. El responsable del tratamiento

La correcta distinción entre los conceptos de responsable y de encargado del tratamiento desempeña un papel fundamental, puesto que permite determinar quién es el responsable del cumplimiento de las normas de protección de datos y cómo los interesados pueden ejercer sus derechos; y también, cómo las autoridades de control pueden llevar a cabo sus tareas de supervisión. Pues bien, el responsable es aquella persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o con otros, determine los fines y medios del tratamiento (art. 4 RGPD, «responsable del tratamiento», siguiendo el anterior art. 2 de la Directiva 95/46/CE, que a su vez lo tomó del Convenio 108 del Consejo de Europa, firmado en 1981).

Lecturas recomendadas

Sobre la figura del responsable del tratamiento, véase:

Grupo de trabajo del artículo 29 (WP29, del inglés *Working Party*) de la Directiva 95/46/CE. Dictamen 1/2010, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», adoptado el 16 de febrero del 2010. *Working Paper* (en adelante, WP) 169.

A. B. Durán (2016). *La figura del responsable en el Derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel*. Madrid: La Ley.

Y anteriormente a estos:

J. M. Busto (2006). «La responsabilidad de los responsables de ficheros de datos personales y de los encargados de su tratamiento». *Revista Aranzadi Civil-Mercantil* (núm. 5, págs. 1-40).

E. del Peso (1994). «La figura del responsable del fichero de datos de carácter personal en la LORTAD». *Informática y derecho: Revista iberoamericana de derecho informático* (núms. 6-7, págs. 249-270).

J. Guerrero (2008). «Artículo 43. Responsables». En: C. Lesmes Serrano (coord.). *La Ley de protección de datos: análisis y comentario de su jurisprudencia* (págs. 625-632). Valladolid: Lex Nova.

La Directiva introdujo algunos cambios con relación al Convenio 108, que reforzaron la figura del responsable del tratamiento:

- La «autoridad controladora del fichero» se sustituyó por el «responsable del tratamiento». Por tanto, ya no se limitaba a un objeto estático, como el fichero, sino a un conjunto de actividades u operaciones que tienen lugar durante el ciclo de información, que empieza con la recogida de información hasta su destrucción.

- Se admite también un control plural, «solo o con otros».

- La exigencia de que el responsable «determine los fines y medios del tratamiento».

- Introduce al «encargado del tratamiento», que no estaba previsto en el Convenio 108 y que veremos a continuación.

Aunque pueda haber una atribución específica por una ley nacional de la facultad de «determinar» los fines y medios del tratamiento, en realidad, la determinación de quién es el responsable se acaba resolviendo gracias a un análisis de los elementos de hecho o de las circunstancias del caso: ¿quién determina las operaciones de tratamiento de datos que presenta el caso? ¿Por qué se produce este tratamiento? ¿Quién lo ha iniciado? Por tanto, a la hora de concretar quién es el responsable del tratamiento, no se atiende a un criterio formal, como sería un nombramiento por ley o por contrato, sino a un concepto funcional, a la realidad de quién se encuentra en condiciones de «determinar» el tratamiento. Así, por ejemplo, en el caso SWIFT, relativo a la transferencia a las autoridades estadounidenses, con fines de lucha contra la financiación del terrorismo, de datos bancarios recogidos por la sociedad SWIFT para la realización de transacciones financieras por cuenta de bancos y entidades financieras, esta se consideró encargada y, en cambio, actuó como responsable. Por tanto, la designación contractual no es decisiva a la hora de establecer su participación, que deriva de las circunstancias concretas de cada caso. Con anterioridad al RGPD, las normas nacionales diferían en cuanto a quién podía ser responsable: la LOPD ha permitido que las entidades sin personalidad jurídica puedan ser responsables en España.

Incluso si los datos se han procesado de manera ilegítima, es importante poder establecer quién es el responsable, para así atribuir las responsabilidades pertinentes. Para ello, el responsable se determinará mediante el Reglamento general de protección de datos, a pesar que pueda también ser titular de derechos de propiedad intelectual, por ejemplo, de acuerdo con otros ámbitos del Derecho. Por ello, se ha considerado que el concepto de responsable es autónomo (WP 169, pág. 10).

Normalmente, el responsable se encuentra en una de las siguientes categorías:

1) Responsable designado mediante una norma explícita: por ejemplo, por medio de un nombramiento de acuerdo con el Derecho nacional o europeo, cosa poco habitual; más habitual suele ser atribuir una responsabilidad pública de la que se desprende la obligación de conservar o facilitar determinados datos personales y, por consiguiente, se deduce la responsabilidad del tratamiento. La Seguridad Social es un ejemplo claro de esto último.

2) Atribución que emana indirectamente de normas jurídicas civiles, mercantiles, laborales, etc. Por ejemplo, el empleador es responsable de los datos personales de los empleados, o la asociación lo es respecto de los datos de los socios. Un ejemplo interesante es el de los operadores de telecomunicaciones.

En principio, los proveedores de servicios de telecomunicaciones solo serán responsables del tratamiento de los datos de tráfico y facturación necesarios para el funcionamiento del servicio de transmisión, pero no de los datos transmitidos en el mensaje.

3) Atribución que emana de las circunstancias de hecho. Para ello, se llevará a cabo una evaluación de las relaciones contractuales entre las partes, y poder así atribuir funciones y responsabilidades. Por tanto, puede darse el caso de que un contrato no designe formalmente a un responsable, pero este pueda derivarse de las funciones atribuidas a cada parte. En caso de duda, pueden tenerse en cuenta otros elementos ajenos a las condiciones de contrato como, por ejemplo, el grado de control real de una de las partes, o la imagen dada a los interesados, o las expectativas que estos tienen.

Las dos primeras categorías, es decir, la atribución formal directa y la indirecta, representan posiblemente la gran mayoría de los casos. Sin embargo, la tercera categoría, basada en las circunstancias de hecho, puede ser imprescindible en algunos casos complejos, pese a que puede llevar en ocasiones a interpretaciones divergentes. Es posible que se planteen un número creciente de casos complejos, en los cuales intermediarios permiten la interacción entre un responsable desarrollador de productos o servicios y el usuario. Este sería el caso, por ejemplo, de las *app stores* para teléfonos inteligentes. No se trata propiamente de responsables, pues no tienen la decisión sobre los fines y medios; al menos no totalmente, aunque pueden establecer directrices a los desarrolladores que incluyan políticas de privacidad. Se ha discutido su posible responsabilidad en tanto que intermediario en el caso de incluir directrices que no respeten la protección de datos, pero también es interesante aprovechar su capacidad para expandir los principios internacionales de protección de datos.

Lectura recomendada

Sobre el papel de las *app stores*, se recomienda leer el siguiente trabajo:

A. Fong (2017). «The role of app intermediaries in protecting data privacy». *International Journal of Law and Information Technology* (núm. 25, págs. 85-114).

Otro aspecto relevante es que, si se designa a un responsable que no puede influir de hecho, ni de derecho, sobre cómo se tratan los datos personales, podrá no ser considerado un responsable (WP169). De hecho, como veremos, la consideración de responsable supone unas responsabilidades que no podrían llevarse a cabo efectivamente en este supuesto. Ciertamente, la determinación de los fines requiere instrucciones precisas, pero puede admitir algún margen discrecional. Por ejemplo, una empresa que contrate campañas de publicidad por correo electrónico puede concretar el material de publicidad que hay que enviar, a quién, cómo debe pagarse, qué cantidades y cuándo. La finalidad del tratamiento incluye elementos esenciales que deben ser decididos por el responsable, como el tiempo de almacenamiento de los datos personales o el acceso a los datos personales, entre otros. En cambio, normalmente no es necesario que se especifiquen los medios técnicos necesarios, como serían los programas informáticos que se van a utilizar. Debe tenerse en cuenta, además, que siempre pueden completarse las indicaciones iniciales asesorando poste-

riormente al encargado en caso de duda. En definitiva, la determinación de los medios solo compete al responsable cuando afecte a elementos esenciales y, en caso contrario, puede ser llevada a cabo por el encargado.

Normalmente, el responsable se presumirá que es la empresa o el organismo público como tal, y no una persona concreta de los mismos, a menos que haya elementos inequívocos que indiquen que el responsable es una persona física. Por ejemplo, una persona física que utilice datos para sus propios fines, fuera del ámbito y control de la empresa u organismo público, será considerada responsable, aunque pudieran eventualmente imputarse también a la empresa responsabilidades por falta de medidas de seguridad. En cambio, no será responsable la persona nombrada por la empresa o el organismo público con el cometido de velar por el cumplimiento del reglamento de protección de datos, es decir, el delegado de protección de datos, sino la propia empresa u organismo público. Ello no obsta a que las leyes nacionales puedan extender la responsabilidad penal a cualquier funcionario o persona física que infrinja la normativa de protección de datos. Veremos también, más adelante, el régimen sancionador del Reglamento general de protección de datos.

Cuando dos o más responsables acuerden conjuntamente los objetivos o los elementos esenciales de los medios del tratamiento, serán considerados corresponsables del mismo[2]. En este caso, los corresponsables determinarán de manera transparente sus respectivas responsabilidades en cuanto al ejercicio de los derechos del interesado, y fijarán sus obligaciones respectivas. La claridad en la asignación de las responsabilidades de cada corresponsable es esencial para evitar que la protección de los datos personales se vea mermada por derechos no garantizados por ninguna de las partes. Las responsabilidades deberán estar, pues, fijadas en un documento escrito en el que se expongan las distintas fases y agentes del tratamiento. Se indicará entonces al responsable del tratamiento competente para el ejercicio de cada uno de los derechos. En este caso, también se tomarán en cuenta las circunstancias de hecho para valorar si el reparto indicado refleja la realidad del tratamiento de datos, para evitar complejidades que escondan falta de responsabilidad.

[2]Una norma con rango de ley puede habilitar el tratamiento de datos personales, y prever al efecto que varias entidades sean corresponsables (art. 26 RGPD y art. 31.2 APLOPD).

Por otra parte, la participación de las partes no tiene que ser necesariamente a partes iguales. Asimismo, no toda cooperación o intercambio de datos entre dos partes que no compartan los fines y los medios supondrá un régimen de corresponsables, sino una transferencia de datos entre responsables que actúan por separado. Eso sí, cuando se cree una infraestructura compartida –por ejemplo, una plataforma común en Internet–, fijando para ello los elementos esenciales de los medios –tipo de datos almacenados, procedimiento de reserva y quién accederá a la información–, entonces serán corresponsables, aunque no compartan los mismos fines. Por otro lado, los corresponsables podrán designar en el acuerdo suscrito un punto de contacto para los interesados. Este acuerdo entre responsables no excluye los derechos que los interesados tengan frente a cada responsable por separado, que siguen vigentes.

Cuando los interesados residan en la Unión, pero no así el responsable, y las actividades consistan en ofertas de bienes o servicios en la Unión, ya sean de pago o gratuitas, o bien en el control del comportamiento de los interesados, el artículo 3.2 del RGPD será de aplicación. En este caso, a menos que el responsable del tratamiento sea una autoridad u organismo público, o bien el tratamiento sea ocasional, no utilice categorías especiales de datos (art. 3.2 RGPD) o datos relativos a condenas e infracciones penales (art. 10 RGPD) o no entrañe un riesgo para los derechos de las personas, el responsable designará a un representante en la Unión Europea (art. 27 RGPD). El representante estará situado en uno de los países de los interesados. El representante atenderá las consultas de las autoridades de control y de los interesados. El interesado podrá emprender también acciones contra el responsable o el encargado.

2.2. El encargado del tratamiento

Como hemos dicho, el encargado del tratamiento no estaba previsto en el Convenio 108. El encargado es aquella persona física y jurídica, autoridad pública, servicio u otro organismo que trate los datos personales por cuenta del responsable (art. 4 RGPD, «encargado del tratamiento»).

Lectura recomendada

J. Leandro (2016). «El encargado del tratamiento». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 321-333). Madrid: Ed. Reus.

El encargado ya estaba previsto en el art. 2e) de la Directiva 95/46/CE y, de manera más detallada, en el art. 12 de la LOPD, y en especial en el Estatuto del encargado del tratamiento, del reglamento de desarrollo. La regulación en el RGPD es amplia, y se incrementan, como veremos, las obligaciones del encargado.

Se trata de una ficción jurídica, según la cual los datos no serían revelados o cedidos a un tercero, sino que siguen bajo la custodia del responsable, pese a ser gestionados por otro (Piñar Mañas, 2008). La obligación de seguir las instrucciones del responsable exime de nueva legitimación al encargado. Esta obligación es la principal diferencia entre las dos figuras. De hecho, si el encargado no sigue las instrucciones del responsable, será considerado responsable (art. 28 RGPD).

Lectura recomendada

J. L. Piñar (2008). «Novedades en relación con la figura del encargado de tratamiento». En: Z. de la Mata (coord.). *Protección de datos: Comentarios al Reglamento* (pág. 219). Lex Nova.

La existencia del encargado depende del responsable: este puede decidir no tratar él mismo los datos por parte de personal autorizado bajo su autoridad directa, sino delegar todas o parte de las tareas de tratamiento a una organización externa. Por consiguiente, así como el responsable es necesario en todo tratamiento, la figura del encargado, o encargados, en cambio, es voluntaria. Puede ser un tratamiento concreto o, por el contrario, general. Además, un responsable puede actuar también como encargado de otro responsable para ciertas operaciones de tratamiento diferentes. Por consiguiente, para que pueda hablarse de un encargado, deben darse tres condiciones básicas:

- Tiene que ser una entidad jurídica independiente del responsable, con o sin personalidad jurídica, de naturaleza privada o pública;

- debe tratar datos personales;

- y, finalmente, debe hacer el tratamiento de datos personales por cuenta del responsable. Este elemento es clave: si establece relaciones con los afectados en su propio nombre, y no así en el del responsable, o si usa los datos para sus propias finalidades, tendrá la consideración de responsable, y esto pese a la existencia de un contrato en el cual conste como encargado (art. 34.2 APLOPD).

Lecturas recomendadas

Para profundizar sobre las condiciones que deben darse para que pueda hablarse de un encargado, conviene leer los siguientes trabajos:

R. García (2010). «Encargado del tratamiento». En: A. Troncoso (dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (págs. 1081-1102). Aranzadi.

F. J. Santamaría (2011). *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*. La Ley.

A. Troncoso (2009). «La huida de la Administración pública hacia el Derecho Privado y la privatización de los servicios públicos: consecuencias en el régimen jurídico de los ficheros de datos personales y en la delimitación del responsable y del encargado del tratamiento». *Anuario de la Facultad de Derecho de Alcalá de Henares* (núm. 2, págs. 31-110).

Cuando se elija a un encargado, es preciso asegurar, eso sí, que este último tenga conocimientos técnicos y medios suficientes para llevar a cabo debidamente el tratamiento.

El tratamiento por parte del encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho europeo o de los estados miembros[3]. Se establecerán en el mismo 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. No parece haber muchas diferencias con el Reglamento de la LOPD. Concretamente, se deberán incorporar las siguientes cláusulas por escrito[4], incluido el formato electrónico (art. 28 RGPD):

- El tratamiento y las transferencias de datos deberán respetar las instrucciones documentadas del responsable, salvo obligaciones impuestas por el Derecho europeo o por un Estado miembro, caso en el que se informará al responsable, a menos que haya razones de interés público que lo prohíban[5].

(3)La necesidad de un contrato ya la recogía el artículo 17.3 de la Directiva 95/46/CE, y la Audiencia Nacional ya se ha pronunciado sobre su importancia (entre otras muchas, sentencia de la AN, Sala de lo Contencioso-administrativo, sección 1.ª, de 16 de febrero del 2005).

(4)La Comisión Europea y las autoridades de control podrán adoptar cláusulas tipo para simplificar el cumplimiento del RGPD. Su utilización será opcional, y de manera alternativa se puede redactar un contrato específico.

(5)Este apartado es confuso y no puede interpretarse en el sentido de que el encargado no informe al responsable de normativa aplicable al tratamiento. Núñez García considera que se refiere más bien a las concretas peticiones de datos cursadas por las autoridades competentes, y al requisito de preservar la confidencialidad de una investigación de una autoridad (Núñez García, 2016, págs. 328-329).

- Se garantizará la confidencialidad por parte de las personas autorizadas a tratar los datos[6].

- Se asistirá al responsable ante las solicitudes en ejercicio de los derechos de los interesados[7].

(6)Esta obligación podría derivar de un contrato, de código deontológico o de un convenio colectivo (Núñez García, «El encargado del tratamiento», 2016, pág. 329).

(7)El encargado tiene la misma obligación que el responsable de designar a un delegado de protección de datos. En las transferencias de datos personales a terceros países, el encargado podrá acreditar que el importador de datos ofrece las garantías adecuadas, a diferencia de la Directiva 95/46/CE, que reservaba esta posibilidad únicamente al responsable.

- Se ayudará al responsable en lo concerniente a la garantía de seguridad de los datos[8].

- Se suprimirán o devolverán los datos, según prefiera el responsable, una vez finalice la prestación de servicios. Igualmente, se borrarán las copias existentes, a menos que el Derecho de la Unión europea o de un Estado miembro requiera su conservación[9].

- Se informará al responsable de todo lo que sea necesario para demostrar el cumplimiento debido de las obligaciones contraídas, y para facilitar la realización de auditorías o inspecciones por parte del responsable o de otro auditor autorizado[10].

- Se informará al responsable si se considera que una instrucción de este contraviene el RGPD u otras normas europeas o de un Estado miembro.

(8)En este sentido, el encargado pondrá en conocimiento del responsable cualquier violación de la seguridad.

(9)El art. 22 LOPD había previsto la posibilidad de conservar los datos a efectos de posibles responsabilidades en las que pudiera incurrir el encargado, una vez finalizada la prestación de servicios.

(10)Se va aquí más allá de lo establecido en la Directiva 95/46/CE, en la línea de lo previsto en la Decisión 2010/87/CE, de 5 de febrero, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, cláusula 5, apartado f). Se permite, así, al responsable llevar a cabo auditorías sobre los tratamientos del encargado. No se menciona, en cambio, la posibilidad de inspecciones por parte de terceros. Por otro lado, la falta de registro de los tratamientos en la autoridad de control se ha trasformado en un registro interno a disposición de esta (art. 30 RGPD).

El encargado tiene discrecionalidad para elegir los medios técnicos y organizativos que considere más adecuados para cumplir su cometido. Puede darse el caso de que el proveedor de servicios encargado del tratamiento elabore un contrato tipo que someta a la firma del responsable. El responsable sigue siéndolo y, por consiguiente, deberá valorar si acepta o no las cláusulas y condiciones del contrato presentado, excluyendo las que, en su opinión, sean contrarias al RGPD. Si no es posible la exclusión, entonces el responsable debería buscar otro proveedor adecuado o, en caso de que no exista, remitir el asunto a las autoridades de control pertinentes.

A veces, la consideración de responsables o encargados puede depender del poder decisorio autónomo que se deje a las partes en el tratamiento de datos. Un ejemplo podrían ser los ensayos clínicos de medicamentos, que ya encontramos en el WP 169 (ejemplo n.º 25). Imaginemos que la empresa Farmacia, S. A. patrocina unos ensayos farmacéuticos y selecciona, para ello, distintos centros de ensayos. De esta manera, Farmacia, S. A. establece el protocolo de

ensayo, indica los requerimientos de protección de datos que hay que tener en cuenta y controla su cumplimiento. Farmacia, S. A. no recoge datos personales directamente, pero sí recibe los de los centros de ensayo y los evalúa e introduce en bases de datos, y también lleva a cabo análisis estadísticos a partir de los mismos. Los centros, por su parte, efectúan los ensayos, facilitan información a los pacientes, facilitan el acceso a documentos y los gestionan y custodian. Por consiguiente, tanto los centros de ensayo como Farmacia, S. A. determinan aspectos importantes del tratamiento de los datos y son corresponsables. Ahora bien, si el margen de decisión del centro fuera mucho más reducido, y dejara a Farmacia, S. A. la determinación de los fines y los elementos esenciales de los medios, entonces los centros serían solo encargados.

2.3. Externalización del servicio y *cloud computing*

Cada vez es más frecuente el hecho de que el responsable externalice el tratamiento a varios encargados del tratamiento. Aquí pueden darse dos situaciones distintas:

- Cada uno de los encargados puede tener una relación directa con el responsable.

- Alguno de los encargados puede ser un subcontratista de un encargado, al cual se le encomienda parte de los cometidos de este último.

El encargado no puede subcontratar el tratamiento o parte del mismo sin la autorización por escrito del responsable[11]. Igualmente, cualquier cambio en la incorporación o sustitución de los subcontratados deberá ser notificado al responsable, que podrá oponerse a los cambios.

Cuando el responsable autorice subcontratar a otro encargado, este último tendrá las mismas obligaciones de protección de datos que el encargado: es decir, deberá acreditar la suficiencia técnica y organizativa. Para demostrar la suficiencia técnica y organizativa, el encargado o, en su caso, el subcontratado, podrán adherirse a un código de conducta. La Comisión o una autoridad de control podrán, asimismo, establecer cláusulas tipo tanto para la regulación de relación del responsable con el encargado, como para la relación con el subcontratado. En caso de incumplimiento por parte del encargado subcontratado (subencargado), el encargado inicial será responsable ante el responsable del tratamiento[12].

(11)Esto significa que no se trata de una auténtica subcontratación libre, ya que siempre requiere el acuerdo del responsable que, además, deberá formalizarse por escrito. El RGPD no los llama subcontratistas, sino «otros encargados», para que quede claro que se les aplica el mismo régimen de obligaciones y derechos.

(12)Se trata de una suerte de responsabilidad solidaria fundada en la culpa *in eligendo* (Núñez García, 2016, pág. 327).

Un supuesto problemático es el *cloud computing*. En este supuesto, hay normalmente varios encargados de la prestación de servicios. Lo realmente complejo, en estos casos, es conocer los detalles del servicio que se contrata y, así, poder identificar correctamente las tareas de cada uno. Por ejemplo, un servicio puede estar a cargo de una empresa que lo ofrezca integrado en una web de servicios de *cloud computing*. El interesado puede pensar entonces que el servicio es prestado directamente por el segundo, cuando puede ser una aplicación de un tercero. En este caso, deberá valorarse la integración y si se proporciona acceso a los datos de los interesados (Durán Cardo, 2015, nota 1367, pág. 524). También plantea dudas el hecho de si la noción de datos personales es aplicable al *cloud computing*. En efecto, la fragmentación, la dispersión de los datos o incluso el cifrado, a veces combinados, podrían evitar la aplicación del RGPD, al no ser ya datos personales. Ahora bien, esto solo sería posible en el supuesto de que los datos proporcionados al proveedor de *cloud computing* no le permitan identificar ni reidentificar a los interesados (Durán Cardo, 2015, pág. 525). Pero esto debe valorarse con cautela. En efecto, el proceso de anonimizar debería ser irreversible, pues en otro caso sería equivalente al uso de seudónimos como medidas de seguridad que deben cumplir plenamente con el RGPD[13]. Tampoco la excepción doméstica o de uso personal es automática en el *cloud computing*[14]. Imaginemos que el cliente de los servicios *cloud* es una persona física que proporciona datos propios, por lo que es el titular de los datos. Podría proporcionar, además, datos de terceros, y entonces será necesario valorar si esta persona física es también responsable respecto de los datos proporcionados al servicio *cloud*. De acuerdo con la jurisprudencia del TJUE, cuando se produzca una difusión de estos datos por Internet y resulten, así, accesibles por un número indeterminado de personas, no podrá aducirse la excepción doméstica o de uso personal[15]. Los proveedores del servicio *cloud* tampoco podrán aducir esta excepción, dada la finalidad con la que tratan los datos.

Lecturas recomendadas

Acerca del tema del *cloud computing*, se recomienda leer los siguientes trabajos:

J. Puyol (2013). *Algunas consideraciones sobre cloud computing*. AEPD.

A. B. Durán (2016). *La figura del responsable en el Derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel*. Madrid: La Ley.

También el elemento funcional, o las circunstancias de hecho, merecen atención en el *cloud computing* para determinar quién fija los fines y los medios del tratamiento. Normalmente, será el propio cliente quien contrata el servicio y decide entregar los datos personales y, por tanto, determina los fines. En cuanto a quién determina los medios, deberemos ver la capacidad de control. Sin embargo, si el proveedor decide utilizar los datos para una finalidad diferente a la prestación del servicio, también será responsable (Durán, 2015, pág. 531). La AEPD y el WP29 consideran generalmente a los clientes como responsables, y a los proveedores, como encargados. La CNIL francesa ha estimado que el proveedor podrá ser considerado como responsable conjunta-

(13)Dictamen 05/2014, del WP29, sobre técnicas de anonimización, adoptado el 10 de abril del 2014 (WP216). Dictamen 05/2012, del WP29, sobre la computación en nube, adoptado el 1 de julio del 2012 (WP196). *Working Paper on Cloud Computing-Privacy and data protection issues*, *Sopot Memorandum*, *International Working Group on Data Protection in Telecommunications*, Sopot (Polonia), 24-04-2012.

(14)Art. 2.2 c) RGPD: «El presente Reglamento no se aplica al tratamiento de datos personales: [...] c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas».

(15)Sentencia del TJUE de 6 de noviembre del 2003, caso *Lindqvist*, C-101/01. En una línea parecida, el WP29 considera que un usuario de una red social podrá llegar a ser considerado también como responsable, ya actúe en nombre de una asociación o empresa, con fines comerciales, políticos o benéficos. El hecho de tener un elevado número de contactos puede ser un indicio al respecto, así como dar acceso general al perfil, más allá de un reducido número de usuarios (Dictamen 05/2009, de 12 de junio, sobre las redes sociales en línea (WP163)). Troncoso (2012b, pág. 72).

mente con el cliente cuando, *de facto*, el cliente no tenga capacidad de decidir. El supervisor europeo también se ha manifestado de manera favorable a la corresponsabilidad. En cuanto a las administraciones públicas, parece más difícil que se pueda traspasar al proveedor del servicio *cloud* el control sobre los fines y los medios del tratamiento[16].

(16)Art. 33 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Lecturas recomendadas

Podéis conocer más a fondo la opinión de los diferentes organismos citados sobre el *cloud computing* y de otras voces autorizadas en el tema en los siguientes trabajos:

AEPD (2013). *Guía para clientes que contraten servicios de Cloud Computing.*

AEPD (2013). *Orientaciones para prestadores de servicios de Cloud Computing.*

CNIL (2012, 25 de junio). *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing* (págs. 5-6).

M. G. Porcedda (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 (eds.). *European Data Protection: in good health?* (págs. 203-232). Springer.

European Data Supervisor (2012, 16 de noviembre). «Opinion of the European Data Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"» (pág. 12).

J. Valero (2012). «La Administración Pública en la nube. Análisis de las implicaciones jurídicas desde la normativa sobre Administración electrónica». En: R. Martínez (ed.). *Derecho y cloud computing* (págs. 231-253). Cizur Menor: Aranzadi.

S. Farré (2010). «El encargado del tratamiento en el ámbito de las Administraciones públicas». En: A. Troncoso (dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (págs. 453-473). Cizur Menor: Aranzadi.

3. Delegado de protección de datos

3.1. Designación de un delegado para la protección de datos

La figura del delegado de protección de datos (DPO, *data protection officer*) no es una novedad absoluta, pues en algunos países como Alemania ya era obligatorio y, en otros como Austria y Holanda, era opcional[17]. Se incorpora al artículo 18.2 segundo guión de la Directiva 95/46, mediante una enmienda presentada por el Parlamento Europeo[18].

Artículo 18.2 Directiva 95/46/CE

«Los estados miembros podrán disponer la simplificación o la omisión de la notificación, solo en los siguientes casos y con las siguientes condiciones:

[...] cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, a un encargado de protección de datos personales que tenga por cometido, en particular:

- hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,
- llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.»

El delegado de protección de datos estaba también presente en el ámbito de las instituciones y organismos europeos[19]. Con la aplicación del Reglamento de protección de datos, va a devenir una figura central para garantizar el cumplimiento del Reglamento en otros países, como España, donde no estaba todavía contemplado. Antes de hablar del RGPD, conviene también mencionar que las autoridades públicas competentes para la prevención, investigación, detección o enjuiciamiento de infracciones penales, salvo que se establezcan excepciones nacionales, deberán también designar a un delegado de protección de datos, en virtud de la Directiva sobre protección de datos personales tratados con fines policiales y judiciales[20].

Lecturas recomendadas

En la doctrina española sobre el Reglamento de protección de datos, pueden mencionarse los trabajos siguientes:

J. R. A. Agustina; A. Blumenberg (2015). «El Data Protection Officer en el marco de la responsabilidad penal de las personas jurídicas». En: *Hacia un Nuevo Derecho Europeo de Protección de Datos*. Valencia: Tirant lo Blanch.

F. J. Santamaría (2011). *El encargado independiente: Figura clave para un nuevo Derecho de protección de datos*. La ley.

(17)La Ley federal alemana de datos personales (BDSG 1977) ya contemplaba el «Beauftragten für den Datenschutz». Tienen también una figura equivalente en Francia, Suecia y Luxemburgo. Fuera del ámbito de la Unión Europea, se prevé una figura similar para el sector público en Estados Unidos (*privacy officers*), o en el sector privado en México (art. 30 de la Ley federal de protección de datos personales en posesión de los particulares, publicada el 5 de julio del 2010), o para los dos sectores en Suiza (art. 11a de la Ley de protección de datos de 1992).

(18)El TJUE ya se pronunció sobre la figura del delegado del artículo 18.2 de la Directiva 95/46/CE en la sentencia (Gran Sala) de 9 de noviembre del 2010, asuntos acumulados C-92/09 y C-93/09, caso*Volker und Markus Schecke y Eifert*.

(19)Artículo 24, apartados uno y ocho de la Directiva 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre del 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Varios documentos del supervisor europeo de protección de datos han analizado este precepto y la figura del delegado de protección de datos.

(20)Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril del 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, que deroga la Decisión marco 2008/977/JAI.

M. Recio (2016). «El delegado de protección de datos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 367-387). Madrid: Ed. Reus.

Por ello, el grupo de trabajo del artículo 29 adoptó en diciembre del 2016 una guía sobre el DPO[21]. No siempre debe existir un DPO; así, el responsable y el encargado del tratamiento designarán obligatoriamente a un delegado de protección de dato en los siguientes casos (art. 37 RGPD[22]):

[21]WP29, *Guidelines on Data Protection Officers* (DPO), adoptado inicialmente el 13 de diciembre del 2016, revisado y adoptado de nuevo el 5 de abril del 2017 (WP243, rev. 01).

[22]La redacción del artículo 35.1 de la propuesta inicial de Reglamento se modificó para evitar cargas excesivas en las pequeñas y medianas empresas. En efecto, se exigía inicialmente a un delegado cuando «[...] b) el tratamiento sea llevado a cabo por una empresa que emplee a doscientas cincuenta personas o más; o c) las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados». Esto fue modificado, como decimos, en la versión final del RGPD.

- Cuando el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales.

- Cuando las actividades principales (*core activities*) requieran una observación habitual y sistemática de los interesados a gran escala.

- Cuando se traten a gran escala categorías especiales de datos personales (art. 9 RGPD) y datos de condenas e infracciones penales (art. 10 RGPD).

- Cuando la designación sea obligatoria, de acuerdo con otras disposiciones de Derecho europeo o de Derecho nacional[23].

[23]Por ejemplo, la designación obligatoria puede venir impuesta por la Directiva sobre protección de datos personales tratados con fines policiales o judiciales.

Lo que deba entenderse por autoridad pública se determinará de acuerdo con la legislación de cada país, que puede contemplar instituciones nacionales, regionales o locales y otras agencias y corporaciones de Derecho público[24]. En todos estos casos, la figura del delegado de protección de datos es obligatoria. Evidentemente, aunque no sea obligatorio, una institución o empresa pueden decidir voluntariamente designar a un DPO[25]. De hecho, el grupo del artículo 29 intenta fomentar una designación voluntaria general de la figura del DPO: por ejemplo, los concesionarios privados de servicios de transporte público, los proveedores de energía o agua, constructoras de infraestructuras viarias, servicios de telecomunicaciones, vivienda pública o corporaciones profesionales[26]. En definitiva, cuando un particular lleve a cabo actividades públicas o actúe como autoridad pública, el grupo del artículo 29 sugiere la designación de un delegado. Y en estos casos, además, este no se limitará a fiscalizar las tareas públicas, sino también la gestión de los datos personales de los empleados, por poner un ejemplo. Sea como fuere, estemos ante un supuesto de designación voluntaria o ante un mandato obligatorio, el DPO deberá cumplir en los dos casos con las obligaciones del Reglamento. El principio de responsabilidad (*accountability*) otorga al DPO un papel relevante, no solo para poder demostrar el cumplimiento del Reglamento general de protección de datos,

sino también para obtener ventaja frente a otras empresas. El DPO tiene, en efecto, un rol de mediador frente a autoridades de supervisión, interesados o simplemente otras unidades empresariales dentro del grupo.

(24)El artículo 37.3 RGPD prevé, asimismo, la posibilidad de que varias autoridades designen a un único delegado de protección de datos para todas ellas, teniendo en cuenta su estructura organizativa y tamaño. De igual manera, los grupos de empresas podrán designar a un único delegado (art. 37.2 RGPD). El art. 35 APLOPD concreta el art. 37 RGPD, e incluye a los colegios profesionales; los centros docentes; las entidades que exploten redes y presten servicios de comunicaciones electrónicas; los prestadores de servicios de la sociedad de la información; algunas entidades de crédito; establecimientos financieros; algunas entidades aseguradoras y reaseguradoras; empresas de servicios de inversión; distribuidores y comercializadores de energía eléctrica; entidades responsables de ficheros comunes para evaluar la solvencia patrimonial; las entidades de investigación y prospección comercial cuando lleven a cabo tratamientos basados en las preferencias o elaboren perfiles de los usuarios; los centros sanitarios; las entidades que emitan informes comerciales de personas o empresas; los operadores de juego electrónico; y las empresas de seguridad privada.

(25)Aunque sea designado voluntariamente, el delegado deberá igualmente cumplir con los requisitos o criterios del reglamento. La AEPD mantendrá una relación actualizada de DPO accesible por medios electrónicos (art. 35.4 APLOPD).

(26)Deberán resolverse las dudas que puedan aparecer sobre el alcance de la obligación de designar a delegados en los supuestos de personas o empresas que gestionen servicios públicos.

En cuanto a la noción de actividades principales, hay que considerarlas de manera amplia. Por ejemplo, ciertamente las actividades principales de un hospital consisten en la atención a los enfermos. Sin embargo, un hospital, para cumplir con este fin, dispondrá de los datos de los historiales médicos de los pacientes. Por ello, la gestión de estos datos se encuentra en la parte principal de actividades de un hospital y, por tanto, deberá designar a un delegado. Lo mismo sucede con una compañía de seguridad privada: su actividad principal consiste en la vigilancia de espacios, y para ello deberá procesar datos personales derivados de las cámaras de vigilancia, entre otros. Por consiguiente, también en este caso deberá designarse a un DPO. En cambio, el solo hecho de gestionar datos para el cobro de las nóminas no es suficiente para considerar obligatorio tener un delegado.

Otro aspecto que hay que considerar es la noción de «tratar a gran escala» datos personales. Por el momento, no existe una cuantificación de esta expresión, y el grupo del artículo 29 considera que deberá concretarla en el futuro. De momento, se indican los elementos siguientes para su correcta consideración[27]:

(27)*Guidelines on Data Protection Officers* (DPOs), adoptadas el 13 de diciembre de 2016, y revisadas y adoptadas de nuevo el 5 de abril de 2017.

- El número de personas afectadas por los datos recopilados, ya sea en porcentaje o como dato cuantitativo.
- El volumen de datos o la diversidad de datos recopilados.
- La duración o permanencia del procesamiento de los datos.
- La extensión geográfica afectada por la actividad.

En este sentido, se considerarán tratamientos a gran escala:

- La recopilación de los datos de los pacientes por parte de un hospital.
- El acopio de datos de viaje mediante tarjetas de transporte.
- El hecho de que un proveedor disponga de los datos de geolocalización de los clientes de una cadena de comida rápida para fines estadísticos.
- Disponer de los datos de los clientes por parte de una compañía de seguros o un banco.
- Procesar los datos de comportamiento por parte de un motor de búsqueda.
- Procesar datos de contenido, tráfico o localización por parte de una compañía telefónica o un proveedor de servicios de Internet.

No serán, en cambio, tratamientos a gran escala que requieran DPO la recopilación de datos de pacientes por parte de un solo médico o de datos criminales por parte de un solo abogado, aunque evidentemente no por el número de afectados, pero sí por el tipo de datos, pueden también llegar a necesitar un delegado de protección de datos.

En cuanto a la noción de «vigilancia regular y sistemática», incluye todas las formas de seguimiento y elaboración de perfiles mediante Internet, como por ejemplo la publicidad basada en el estudio del comportamiento del cliente (*behavioural advertising*). La regularidad de la actividad de seguimiento o vigilancia requiere continuidad, aunque pueda ser periódica, así como repetición y constancia. Por otro lado, se considerará como sistemático el seguimiento cuando se base en un modelo o sistema, cuando esté prefijado u organizado, cuando forme parte de un plan más general o de una estrategia general. Por ejemplo, quedarán dentro de esta expresión las actividades de las redes de comunicaciones; los perfiles de crédito; seguros; prevención de fraudes; detección de blanqueo de moneda; geolocalización; estudios de comportamiento de usuarios; seguimiento de datos corporales en aparatos como relojes inteligentes; cámaras de circuito cerrado; medición inteligente y coches inteligentes; domótica, etc. En cuanto a las «categorías especiales de datos o a los datos relativos a condenas e infracciones penales», su contenido no parece plantear mayores problemas.

En algunos casos, el responsable del tratamiento no deberá designar a un delegado, mientras que el encargado sí deberá hacerlo: imaginemos una empresa familiar que contrata los servicios de una empresa de análisis de navegación web, perfil de consumo y marketing. El responsable, la empresa familiar, claramente no procesa datos a gran escala, pero en cambio las actividades del encargado, que tiene a muchas pequeñas empresas como clientes, sí que entran

en el supuesto del artículo 37 RGPD. Como medida de buenas prácticas, el delegado del encargado también deberá supervisar aspectos de logística, información y recursos humanos en los que actúe como responsable de los datos.

Las cualidades profesionales del delegado incluyen un conocimiento especializado en Derecho nacional y europeo de protección de datos, y una práctica en esta materia que le permita cumplir con sus cometidos. Pueden, por consiguiente, ser profesionales del Derecho, aunque no parece excluirse por ahora la posibilidad de que otros profesionales adquieran conocimientos jurídicos complementarios para poder ser designados como delegados[28]. El grupo del artículo 29 aconseja que las autoridades de supervisión organicen cursos de formación y ofrezcan guías para los DPO. Además, puede ser útil tener conocimiento del sector empresarial y de la organización corporativa: al menos, las operaciones principales, el sistema de información, la seguridad de los datos y la protección de datos personales necesarios en la empresa. En el caso de administraciones públicas, el delegado deberá conocer los procedimientos administrativos principales de la organización en la cual se encuentre. En cuanto a las cualidades personales, serán imprescindibles la integridad y ética profesional en el cumplimiento del RGPD. El delegado deberá fomentar una cultura de la protección de datos en su organización, y facilitar el cumplimiento de los principios y derechos reconocidos en el RGPD, así como ayudar a la protección mediante diseño o por defecto, que veremos más adelante. Asimismo, deberá contribuir a un correcto almacenamiento de los datos, a su protección y a las notificaciones en caso de brechas de seguridad. El nivel de conocimientos en protección de datos dependerá de las tareas concretas requeridas en el caso concreto. Así, cuanto mayor sea la cantidad, complejidad y porcentaje de datos sensibles, el delegado deberá tener un mayor conocimiento experto y apoyo. Otro aspecto que hay que considerar es el volumen y la frecuencia de las transferencias de datos personales de la empresa hacia fuera de la Unión Europea.

[28]La AEPD ha sido la primera en aprobar un esquema de certificación de delegados de protección de datos (Esquema AEPD-DPD), el 10 de julio del 2017, con indicación de los criterios para la certificación, así como los requisitos de las entidades certificadoras.

Lectura recomendada

En cuanto a la designación como delegado, Miguel Recio considera que el delegado debería ser una persona con una sólida formación jurídica. Podéis profundizar más en el tema leyendo su trabajo:

M. Recio (2016). «El delegado de protección de datos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 367-387). Madrid: Ed. Reus.

La figura del delegado puede tratarse de algún trabajador de la plantilla del responsable o del encargado, aunque esto no es imprescindible, o puede estar vinculado por un contrato de servicios[29]. En este último caso, será imprescindible que no exista ninguna situación de conflicto de intereses. Pueden también combinarse diferentes perfiles en un equipo para cumplir con la totalidad de tareas encargadas al delegado[30]. En este supuesto, será necesario clarificar las tareas encargadas a cada miembro del equipo y elegir a un representante para los interesados, o una persona visible para cada interesado. Esto debería figurar en el contrato de servicios. Por otro lado, el hecho de tener a un delegado no impide contar, asimismo, con auditores externos de protección de datos. Eso sí, deberán identificarse con precisión los cometidos de uno y otro para

[29]En el documento relativo a la evaluación de impacto de la Comisión Europea sobre la propuesta de Reglamento, de 25 de enero del 2012, se define al delegado como «una persona responsable, en el seno de un responsable del tratamiento o de un encargado del tratamiento, de supervisar y controlar de manera independiente la aplicación interna y el respeto de las normas sobre protección de datos. El DPO puede ser tanto un empleado interno como un consultor externo» (traducido del inglés).

evitar solapamientos o, por el contrario, lagunas en las responsabilidades de uno y otro. En todo caso, debe quedar claro que el consultor o auditor externo no es un delegado. El responsable o el encargado deberán publicar sus datos de contacto y se comunicarán asimismo a la autoridad de control. El DPO no responde personalmente en caso de incumplimiento con el Reglamento, algo que corresponde al responsable del tratamiento de los datos o al encargado. De hecho, son estos últimos los que deben facilitar el cumplimiento de las tareas encomendadas al delegado. Como veremos, las tareas del delegado lo convierten en una suerte de gestor del gobierno de los datos.

(30)El delegado de protección de datos puede integrarse en un equipo multidisciplinar con otros profesionales como, por ejemplo, un responsable de seguridad (CSO, *chief security officer*), un responsable de cumplimiento (*compliance officer*) o un encargado de los datos (CDO, *chief data officer*).

Un grupo empresarial puede designar a un delegado único, siempre que este sea fácilmente accesible. Esto significa que el DPO debe poder llevar a cabo eficazmente las tareas como punto de contacto de los interesados. En este sentido, es importante que los datos de contacto se encuentren disponibles. Otro aspecto destacable es que la comunicación se hará en la lengua de la autoridad de supervisión y de los interesados. De igual manera, varias autoridades u organismos públicos podrán designar a un único delegado de protección de datos, al cual se le aplica lo dicho anteriormente. Cuando un responsable o encargado represente a categorías de responsables o encargados, podrá designar a un delegado que actúe por cuenta de estas asociaciones.

3.2. Posición del delegado

El responsable o el encargado deberán publicar los datos de contacto del delegado para que los interesados puedan acceder al mismo. Además, estos datos de contacto serán comunicados a la autoridad de supervisión. El objetivo es conseguir que tanto en el funcionamiento ordinario interno, como desde fuera de la empresa, se pueda acceder al DPO directa y confidencialmente, sin tener que pasar primero por la organización corporativa[31]. En este sentido, se incluirá información de contacto como dirección postal, número de teléfono y correo electrónico. Cuando se considere conveniente, se podrá completar la información anterior con una página web o un acceso desde la web corporativa. No es imprescindible que se incluya el nombre del delegado, y serán el responsable y el mismo DPO los que lo consideren conveniente. Se recomienda informar al menos a los empleados de la empresa y a la autoridad supervisora del nombre y de los datos de contacto del delegado[32].

(31)Acudir al delegado para asesorarse y asegurar el cumplimiento de las responsabilidades del responsable y del encargado debe ser el procedimiento estándar (Recio, 2016, pág. 381).

(32)El GT29 indica que las eventuales comunicaciones se harán en el idioma o idiomas de las autoridades de control y los interesados.

El responsable y el encargado deberán garantizar que el delegado se involucre desde la primera fase posible en la protección de los datos. Por ejemplo, el DPO debe participar en la elaboración de los informes de impacto, que veremos más adelante. Esta es la perspectiva que puede permitir un mejor cumplimiento del RGPD y del principio de privacidad mediante el diseño (*privacy by design*). El delegado debe, así, tomar parte en los grupos de discusión para los cuales el tratamiento de datos sea relevante. De hecho, al igual que el CIO (*chief information officer*), el DPO debe participar también de manera habitual en las reuniones de gestión de la empresa. Para que pueda hacer su cometido

con eficacia, debe proporcionársele a su debido tiempo toda la información relevante para el tratamiento de datos. En el caso de no seguir las indicaciones del delegado, deberían documentarse los motivos para ello. Igualmente, hay que informar al delegado en el caso de fallo de seguridad.

El delegado deberá disponer de apoyo por parte del equipo directivo. Además, tendrá que disponer de tiempo suficiente para llevar a buen puerto sus tareas. Esto es particularmente importante cuando su función es a tiempo parcial o la combina con otra. Para ello, pueden establecerse porcentajes de dedicación para que no resulte perjudicada la función de protección de datos. Otro aspecto crucial es la necesidad de dotar al DPO de recursos financieros, infraestructuras y, si fuera necesario, un equipo de profesionales adecuado a sus funciones. En este último supuesto, se detallarán las funciones y responsabilidades de cada miembro del equipo. Debe comunicarse su nombramiento oficial para que pueda ponerse en contacto con toda la organización, si fuera necesario. Debe poder acceder a los departamentos de recursos humanos, informáticos, legales y de seguridad. Además, debe poder seguir una formación continuada y acceder, en lo posible, a foros y talleres de protección de datos.

El delegado no debe recibir ninguna instrucción en lo que respecta al desempeño de sus funciones, y rendirá cuentas al más alto nivel jerárquico del responsable o del delegado[33]. En este sentido, no se le indicará cómo debe resolver un problema o investigar una queja o si debe consultar o no a la autoridad de supervisión. Tampoco debe recibir indicaciones sobre cómo tiene que interpretar el RGPD. Eso sí, los responsables finales son el responsable del tratamiento y el encargado, que pueden disentir. En este caso, el delegado debe poder manifestar su posición de disenso si cree que la decisión del responsable es contraria al RGPD. Otro aspecto conectado es la posibilidad, o no, de destituir o sancionar al delegado por el cumplimiento de sus funciones. Evidentemente, las sanciones prohibidas son aquellas que derivan exclusivamente del funcionamiento de su cometido; se permite, claro está, la destitución del delegado por hurto, acoso sexual u otras faltas graves. Sería, en cambio, una sanción indebida el supuesto en el cual un delegado considera conveniente la realización de un informe de impacto cuando el responsable no está de acuerdo, y este último lo destituye por este motivo[34]. Tampoco puede perjudicarse al delegado dilatando su promoción o impidiendo el acceso a los beneficios generales de otros trabajadores, como cursos u horarios de verano.

(33)Es decir, solo reportará a la autoridad que les designa, no a un superior directo (supervisor europeo de protección de datos, 2005).

(34)El art. 37.2 APLOPD exige dolo o negligencia grave en el ejercicio de sus funciones.

Además, el delegado estará sujeto al deber de secreto y confidencialidad en lo relativo a sus tareas. Esto no impide al DPO contactar y pedir consejo a la autoridad supervisora. Ahora bien, en el ejercicio de sus funciones, el DPO podrá acceder a los datos personales y procesos de tratamiento, y el responsable o el encargado no podrán oponer a este acceso ningún deber de confidencialidad o secreto (art. 37.4 APLOPD). Por otro lado, los interesados podrán ponerse en contacto con el delegado en el ejercicio de sus derechos, y el delegado deberá mantener el secreto o la confidencialidad sobre los datos conocidos, por

razón del ejercicio de su cargo. El responsable o el encargado velarán por la no existencia de conflictos de intereses en el ejercicio de sus funciones. Esto minaría la posición independiente del delegado, imprescindible para cumplir debidamente con sus funciones. Por ejemplo, si el DPO no ejerce sus funciones a tiempo completo, sino que, por el contrario, combina su cargo con otro en la empresa, debe valorarse si su otro cometido no entra en conflicto con la función de delegado. Podría ser una buena práctica para los responsables o encargados:

- Identificar los cargos en la empresa que resultan incompatibles con la función de delegado.
- Establecer reglas internas al respecto, para evitar conflictos de intereses.
- Declarar que el DPO no tiene conflictos de interés, para que se tome conciencia de la importancia de este punto.
- Debe tenerse en cuenta que el conflicto de interés puede ser distinto en función de si el DPO es elegido en la empresa o fuera de ella.

3.3. Funciones del delegado

De acuerdo con el artículo 39 RGPD, el delegado tendrá como mínimo las funciones que se mencionan a continuación:

- Recabar información para identificar los tratamientos de datos.
- Supervisar el cumplimiento del RGDP y otras disposiciones de protección de datos. Esto incluye la asignación de responsabilidades, la concienciación y la formación del personal y las auditorías.
- Informar y asesorar al responsable, al encargado y a los empleados responsables del tratamiento de datos. Por ejemplo, el artículo 37.5 APLOPD impone el deber de comunicar al responsable o al encargado cuando el DPO aprecie la existencia de una infracción relevante.
- Asesorar sobre la evaluación de impacto relativa a la protección de datos.
- Actuar como punto de contacto y cooperar con la autoridad de control, por ejemplo, mediante una consulta previa después de una evaluación de impacto que muestre un alto riesgo. De acuerdo con el art. 38.1 APLOPD, el afectado, antes de acudir a la AEPD o a las autoridades autonómicas de protección de datos, se dirigirá al DPO. La decisión del DPO deberá darse en el plazo máximo de dos meses desde la presentación de la reclamación. Si el afectado no se dirige primero al DPO, la AEPD o la autoridad de protección de datos autonómica podrá remitir la reclamación al DPO para que

resuelva sobre la misma en el plazo de un mes. En ausencia de respuesta, la autoridad de protección de datos continuará el procedimiento (art. 38.2 APLOPD).

Aunque, de acuerdo con el artículo 35 RGPD, es el responsable y no el delegado el que debe llevar a cabo un hipotético informe de impacto sobre la protección de datos (*data protection impact assessment*, DPIA), el DPO tiene un importante cometido a la hora de asesorar al responsable. El responsable debería buscar el asesoramiento del delegado, según el grupo 29, en los siguientes casos:

- Decidir si debe o no hacerse el DPIA.
- Sobre la metodología para llevarlo a cabo.
- Sobre si es conveniente que lo haga un auditor externo.
- Qué garantías técnicas, organizativas y de otro tipo deben tenerse en cuenta para evitar vulnerar derechos de los interesados.
- Validación del DPIA y respeto del mismo al RGPD.

En caso de no seguir las indicaciones del delegado, el DPIA tendrá que especificar los motivos para ello. En el DPIA, se pueden incluir las tareas que deberá hacer el delegado.

De manera general, el delegado tendrá que priorizar, en su tarea de supervisión, las actividades de tratamiento que supongan mayor riesgo. Se trata, por consiguiente, de una perspectiva pragmática, basada en la prevención de riesgos (*risk-based approach*), que se concreta en la selección de la metodología para hacer el DPIA, qué aspectos requieren una auditoría externa, qué formación deben tener los empleados que lleven a cabo tratamiento de datos y en qué actividades hay que concentrar más recursos.

El DPO llevará un registro o inventario de sus actividades, así como de todas las actividades de tratamiento de datos del responsable. La lista de funciones del delegado puede ser ampliada por el responsable y, de esta manera, puede encargarse del registro de actividades corporativas no directamente relacionadas con el tratamiento de datos. Sea como sea, el registro debe permitir al responsable y a la autoridad de supervisión valorar el correcto cumplimiento del RGPD.

3.4. Control externo del cumplimiento del marco legal

El responsable puede encargar a un empleado, o bien a un auditor autorizado, la realización de auditorías o inspecciones. El encargado deberá permitir y contribuir a la ejecución de estas auditorías. El delegado de protección de datos podrá colaborar en la formación de los auditores.

La autoridad de control competente podrá adoptar normas corporativas vinculantes, que incluirán mecanismos de verificación del cumplimiento mediante auditorías de protección de datos (art. 47.2j RGPD). De hecho, dentro de los poderes de cada autoridad de control, se menciona la facultad de llevar a cabo investigaciones en forma de auditorías de protección de datos (art. 58b RGPD).

Bibliografía

AEPD (2013). *Guía para clientes que contraten servicios de Cloud Computing*.

AEPD (2013). *Orientaciones para prestadores de servicios de Cloud Computing*.

Agustina, J. R. A.; Blumenberg, A. (2015). «El Data Protection Officer en el marco de la responsabilidad penal de las personas jurídicas». En: *Hacia un Nuevo Derecho Europeo de Protection de Datos*. Valencia: Tirant lo Blanch.

Busto, J. M. (2006). «La responsabilidad de los responsables de ficheros datos personales y de los encargados de su tratamiento». *Revista Aranzadi Civil-Mercantil* (núm. 5, págs. 1-40).

CNIL (2012, 25 de junio). *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing*.

Durán, A. B. (2016). *La figura del responsable en el Derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel*. Madrid: La Ley.

European Data Supervisor (2012, 16 de noviembre). «Opinion of the European Data Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"» (pág. 12).

Farré, S. (2010). «El encargado del tratamiento en el ámbito de las Administraciones públicas». En: A. Troncoso (dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (págs. 453-473). Cizur Menor: Aranzadi.

Fong, A. (2017). «The role of app intermediaries in protecting data privacy». *International Journal of Law and Information Technology* (núm. 25, págs. 85-114).

García, R. (2010). «Encargado del tratamiento». En: A. Troncoso (dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (págs. 1081-1102). Aranzadi.

Guerrero, J. (2008). «Artículo 43. Responsables». En: C. Lesmes (coord.). *La Ley de protección de datos: análisis y comentario de su jurisprudencia* (págs. 625-632). Valladolid: Lex Nova.

Grupo de trabajo del artículo 29 de la Directiva 95/46/CE. Dictamen 1/2010, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», adoptado el 16 de febrero de 2010 (WP 169).

Hernández, J. M. (2013). *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*. Cizur Menor: Aranzadi.

Martínez, R. (2012). «El complejo encaje normativo de la propuesta de Reglamento general de protección de Datos de la Unión Europea». *Actualidad Jurídica Aranzadi* (núm. 839).

Núñez, J. L. (2016). «El encargado del tratamiento». En: José Luis Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 321-333). Madrid: Ed. Reus.

Peso, E. del (1994). «La figura del responsable del fichero de datos de carácter personal en la LORTAD». *Informática y derecho: Revista Iberoamericana de Derecho Informático* (núms. 6-7, págs. 249-270).

Piñar, J. L. (2008). «Novedades en relación con la figura del encargado de tratamiento». En: Zabía de la Mata (coord.). *Protección de datos: Comentarios al Reglamento* (pág. 219). Lex Nova.

Porcedda, M. G. (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 (eds.). *European Data Protection: in good health?* (págs. 203-232). Springer.

Puyol, J. (2013). *Algunas consideraciones sobre cloud computing*. AEPD.

Rallo, A.; García, R. (ed.) (2015). *Hacia un nuevo derecho europeo de protección de datos* (*Towards a new European data protection regime*) (págs. 29-81).Valencia: Tirant lo Blanch.

Recio, M. (2016). «El delegado de protección de datos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 367-387). Madrid: Ed. Reus.

Santamaría, F. J. (2011). *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*. La Ley.

Supervisor europeo de protección de datos (2005, 28 de noviembre). *Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001*. Bruselas.

Troncoso, A. (2009). «La huida de la Administración pública hacia el Derecho Privado y la privatización de los servicios públicos: consecuencias en el régimen jurídico de los ficheros de datos personales y en la delimitación del responsable y del encargado del tratamiento». *Anuario de la Facultad de Derecho de Alcalá de Henares* (núm. 2, págs. 31-110).

Troncoso, A. (2012a). «Hacia un nuevo marco jurídico europeo de protección de datos personales». *Revista Española de Derecho Europeo* (núm. 43, págs. 25-184). Cizur Menor: Aranzadi.

Troncoso, A. (2012b). «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una». *IDP, Revista de Internet, Derecho y Política* (núm. 15).

Valero, J. (2012). «La Administración Pública en la nube. Análisis de las implicaciones jurídicas desde la normativa sobre Administración electrónica». En: Ricard Martínez (ed.). *Derecho y cloud computing* (págs. 231-253). Cizur Menor: Aranzadi.