Tutela judicial, responsabilidad y sanciones

PID_00250225

Antoni Roig

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Antoni Roig

Índice

1. Derecho de reclamación ante la autoridad de control

Aunque existían en la Directiva 95/46/CE los derechos a presentar reclamaciones y a la tutela judicial, el derecho expreso a presentar reclamaciones ante la autoridad de control es una novedad del RGPD[1] (Recio, 2016). La jurisprudencia de aplicación de la citada Directiva ha servido para dar lugar a las previsiones del RGPD[2].

(1)El art. 28, apartado 4 de la Directiva 95/46/CE otorgaba a las autoridades de control el poder de atender reclamaciones de los interesados en relación con el tratamiento de sus datos personales.

(2)STJUE (Sala Tercera) de 1 de octubre del 2015. Caso Weltimmo, C-230/14; STJUE (Gran Sala) de 6 de octubre del 2015. Caso Schrems, C-362/14.

Lectura recomendada

M. Recio (2016). «Los derechos a presentar reclamaciones ante la autoridad de control y a la tutela judicial efectiva». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 539-553). Madrid: Ed. Reus.

De acuerdo con el art. 77 RGPD, cualquier persona tiene derecho a presentar una reclamación ante una autoridad de control si considera que el tratamiento de datos personales que le conciernen infringe el RGPD[3]. Como veremos, esto no es impedimento para la posibilidad de interponer, igualmente, otros recursos ante los tribunales. Es decir, con carácter general, el interesado puede presentar recursos administrativos y hacer uso de mecanismos extrajudiciales ante la autoridad de control, o bien interponer una acción judicial ante el tribunal competente.

(3)Considerando 141 del RGPD. La reclamación puede hacerla incluso otra persona que no sea el interesado. De hecho, en algunos casos, por razón del cargo que se ocupa, se tiene la obligación de acudir a la autoridad de control. Carles San José, en su ponencia en el Ciclo de conferencias sobre el RGPD, organizado por la APDCAT, decía que el art. 77 RGPD no impide que la reclamación la pueda hacer cualquier otro sujeto a parte del interesado. Podéis ver la sesión del 9 de marzo de dicho ciclo en: «Cicle RGPD, 5a. Jornada. Garanties per a una protecció efectiva del dret a la protecció de dades».

La autoridad de control a la que se debe presentar la reclamación será, en principio, la del Estado miembro donde el interesado tenga su residencia o lugar de trabajo, o donde se haya cometido la supuesta infracción (art. 77, primer apartado, del RGPD). En el caso Schrems, el TJUE ya afirmó que la reclamación del interesado puede versar sobre cualquier tratamiento que este considere que vulnera su derecho a la protección de datos (podéis ver nota 2, apartado 55 de la sentencia). Por otro lado, las normas corporativas vinculantes y los representantes deberán indicar este derecho a presentar una reclamación ante las autoridades de control[4].

(4)Art. 47, apartado 2e RGPD; y los artículos relacionados con el principio de transparencia y derecho de información, art. 12, apartado 4 del RGPD; art. 13, apartado 2d RGPD; y art. 15.1f9 RGPD

Una parte importante de la nueva regulación sobre las reclamaciones ante las autoridades de control se refiere a las competencias, funciones y obligaciones de las mismas. En cuanto a las competencias, se establece el criterio de la autoridad principal, que obliga a la cooperación entre autoridades de control[5] (art. 56 RGPD). La función de las reclamaciones queda definida en el art. 57 RGPD (art. 57, apartado 1f RGPD). La autoridad de control deberá informar

(5)En cuanto a la cooperación, art. 60 RGPD. La cooperación con autoridades de control de países terceros o con organizaciones internacionales puede verse en el art. 50b RGPD.

al interesado sobre la tramitación de su reclamación y el resultado final[6]. Asimismo, la autoridad de control deberá indicar la posibilidad de recurso ante los tribunales frente a la decisión de la autoridad de control. En el art. 65 APLOPD, se prevé que no se iniciará el procedimiento en el supuesto de que el responsable o encargado, previa advertencia, haya adoptado medidas correctivas, siempre que no se haya causado perjuicio al afectado y las medidas garanticen plenamente sus derechos. La AEPD inadmitirá las reclamaciones cuando no versen sobre cuestiones de protección de datos, carezcan de fundamento, sean abusivas o no aporten elementos que permitan investigar la supuesta vulneración de derechos. Antes de iniciar el procedimiento, la AEPD podrá llevar a cabo tareas de investigación durante un plazo máximo de un año, cuando la reclamación verse sobre los derechos reconocidos en los arts. 15 a 22 RGPD (art. 68 APLOPD). La AEPD podrá acordar medidas provisionales e incluso pedir el bloqueo de los datos, la cesación de su tratamiento y, en caso de incumplimiento, proceder a su inmovilización, cuando considere que el tratamiento puede suponer un menoscabo grave a los derechos del afectado (art. 69.2 APLOPD).

(6)Puede haber aspectos reservados por razón del procedimiento, que no se podrán facilitar al interesado.

2. Derecho a la tutela judicial

1) Reglas generales de competencia

El interesado, de manera independiente de que haga uso o no de la facultad de presentar un recurso administrativo u opte por una resolución extrajudicial de conflictos, tiene también derecho a presentar un recurso contra los responsables, directamente ante los tribunales, por infracción del RGPD[7]. Los tribunales competentes serán los del Estado miembro donde el responsable o el encargado tengan un establecimiento (art. 79, apartado 2 RGPD). El interesado podrá optar también por los tribunales del Estado miembro en el cual tenga su residencia habitual. Ahora bien, si el responsable o el encargado son una autoridad pública con poderes públicos, será el Estado miembro de la misma el competente.

Por otro lado, el Reglamento amplía las previsiones del derecho al recurso judicial, pues la decisión jurídicamente vinculante de una autoridad de control, de rechazo o desestimación puede ser también recurrida ante los tribunales del Estado miembro de la autoridad de control (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2014, pág. 134). De igual manera, si una autoridad competente, de acuerdo con los arts. 55 y 56 RGPD, no resuelve la reclamación o no informa al interesado sobre la tramitación de la misma, pasados tres meses el interesado tendrá derecho a tutela judicial frente a la autoridad de control[8]. La tutela judicial ante los tribunales no impide la posibilidad complementaria de recurso administrativo o extrajudicial[9] (art. 78, apartados 1 y 2 RGPD). Las acciones judiciales se plantearán en el mismo Estado miembro donde se encuentre la autoridad de control (art. 78, apartado 3 RGPD).

2) Procedimiento

El ejercicio de la reclamación puede hacerse directamente, o bien delegarse a un representante. En este último supuesto, el interesado deberá dar un mandato a una entidad, organización o asociación sin ánimo de lucro, legalmente constituida, cuyos objetivos sean de interés público y que actúe en el ámbito de la protección de datos. De esta manera, el representante podrá actuar y ejercer los derechos del interesado. De hecho, un Estado miembro podrá prever en su ordenamiento nacional que el representante pueda también presentar una reclamación ante la autoridad de control, en caso de vulnerarse los derechos del interesado contemplados en el RGPD.

(7)Ya en el art. 22 y en el considerando 55 de la Directiva 95/46/CE. Anteriormente, llegó a ser únicamente considerado un derecho complementario (Recio, 2016, apartado 5). El derecho a la tutela judicial se encuentra también en la Carta de los Derechos Fundamentales de la Unión Europea y, por tanto, la interpretación del RGPD en este punto deberá hacerse a la luz de la Carta, lo que ya fue afirmado por el TJUE en relación con la Directiva 95/46/CE (Recio, 2016, pág. 549).

(8)El interesado recurrirá la decisión de la autoridad de control en el mismo Estado miembro en el que se presentó la reclamación, incluso si no se corresponde con su residencia. Por ejemplo, ya en el caso Schrems, el reclamante, aunque era austríaco, presentó su reclamación ante la autoridad de control irlandesa y, posteriormente, interpuso recurso ante los tribunales de este país.

(9)En este sentido, se puede preferir primero un mecanismo más rápido, antes de acudir al órgano jurisdiccional competente.

En el supuesto de que llegue a conocimiento de un tribunal competente la pendencia ante un tribunal de otro Estado miembro de un procedimiento sobre el mismo asunto y responsable o encargado, el primero se pondrá en contacto con el segundo. El tribunal competente podrá entonces suspender su procedimiento en favor del tribunal ante el cual se ejercitó la acción en primer lugar. Si el procedimiento está pendiente en primera instancia, frente a un tribunal competente ante el que se ejercitó la acción en primer lugar, entonces los demás tribunales podrán inhibirse para acumular eventualmente las acciones.

3. Responsabilidad penal, civil y administrativa

1) Responsabilidad penal

Los supuestos en los que el responsable puede incurrir en responsabilidad penal por el tratamiento de los datos personales se encuentran en el artículo 197 del Código penal (Agustina y Blumenberg, 2015; López, 2016). En el segundo apartado, se prevén penas para quienes accedan, se apoderen, utilicen o modifiquen, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro, que se encuentren en ficheros, soportes electrónicos o archivos o registros privados o públicos. Se trata de un delito doloso, con ánimo de vulnerar la privacidad y apoderarse de la información para beneficiarse o causar daño. Las penas aumentan en el apartado 3 del art. 197 CP, cuando se difunde la información. Igualmente, se castiga la difusión de información cuando se conozca su origen ilícito, aunque no se haya accedido a ella personalmente.

Lecturas recomendadas

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.

L. F. López (2016). «La responsabilidad del responsable». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 275-294). Madrid: Ed. Reus.

Pues bien, por cuanto aquí interesa, los responsables y encargados pueden incurrir igualmente en estos tipos penales, de modo que se aumente la pena correspondiente[10]. También se prevén penas en su mitad superior si se difunden los datos, cuando se trate de datos especiales, cuando haya ánimo de lucro o cuando lo haga personal al servicio de las administraciones públicas (art. 198 CP). Finalmente, el art. 197 *quinquies* prevé la posibilidad de que una persona jurídica sea responsable de estos supuestos. Esto podría ser relevante en supuestos de empresas de *cloud* que no borrasen los datos de un cliente una vez finalizada su relación de servicio con él.

[10]Art. 197.4 CP: se aumenta hasta los cinco años la pena en el caso de ser el responsable o el encargado quienes incurran en los tipos del art. 197.1 y 197.2 CE.

2) Responsabilidad civil

Toda persona que haya sufrido daños y perjuicios materiales por el incumplimiento no solo del RGPD, sino también de normas de desarrollo europeo y nacional, podrá reclamarlos al responsable o al encargado[11]. La responsabilidad civil de los responsables y encargados responde a una finalidad distinta de las sanciones administrativas que imponen las autoridades de control (Nieto, 2016, págs. 556-557). Así, la sanción administrativa, que veremos más adelante, es una manifestación de *ius puniendi* del Estado y tiene una finalidad

[11]Art. 82 RGPD, y ya en el art. 23 de la Directiva 95/46/CE podemos encontrar un mandato al legislador para que reconociera este derecho, que en España se concretó en el art. 19 LOPD (Nieto, 2016).

preventiva. La responsabilidad civil, en cambio, tiene por finalidad resarcir de un perjuicio sufrido. Los principios del sistema de responsabilidad del art. 82 RGPD (Nieto, 2016, págs. 558-566) son:

- La protección uniforme y de obligado cumplimiento para los Estados (considerando 10 del RGPD) frente a una actividad fáctica o jurídica o la inactividad del responsable[12] (art. 82, apartado segundo del RGPD).
- La responsabilidad directa del responsable (art. 82 RGPD).
- La responsabilidad subjetiva, es decir, con dolo, culpa o negligencia (incluye la culpa *in vigilando*) que puede exonerarse de acuerdo al art. 82.3 RGPD. En España, la responsabilidad patrimonial de la Administración Pública sigue, en cambio, un sistema de responsabilidad objetiva.
- La reparación integral, incluyendo los daños morales (considerando 146 del RGPD).
- La responsabilidad extracontractual, es decir sin que medie necesariamente un contrato entre el titular de los datos y el responsable.
- La responsabilidad solidaria para garantizar una indemnización efectiva (apartados 4 y 5 del art. 82 RGPD).
- La acción de reclamación de responsabilidad por daños (art. 82,6 RGPD y art. 79.2 RGPD).

[12] La infracción no se reduce al RGPD, sino también a los actos delegados y de ejecución adoptados de acuerdo con el RGPD, así como las normas nacionales (considerando 146 RGPD).

Lectura recomendada

E. Nieto (2016). «Derecho a indemnización y responsabilidad». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 555-570). Madrid: Ed. Reus.

El responsable responderá de los daños y perjuicios causados por tratamientos que incumplan el RGPD. El encargado únicamente responderá por daños y perjuicios cuando específicamente incumpla obligaciones prevista en el RGPD y dirigidas concretamente al encargado. Asimismo, también responderá por daños y perjuicios cuando haya actuado al margen de las instrucciones, estas sí legales, del responsable. Para poder responder, el interesado deberá acreditar que existe daño[13], y que la causa del perjuicio creado está directamente relacionada con el responsable o el encargado. La obligación de acreditar que las actuaciones del responsable y del encargado respetan el RGPD invierte la carga de la prueba, de manera que el interesado no deberá demostrar la culpa o negligencia del responsable, sino que será este último quien deberá acreditar que su conducta es diligente (Vilasau y Vila, 2010, pág. 215; López, 2016, págs. 280-281).

[13] No hay, pues, presunción de existencia de perjuicio cuando se acredite la infracción del RGPD.

Lectura recomendada

M. Vilasau; M. A. Vila (2010). «Intimidad y datos personales en Internet». En: M. Peguera (coord.). *Principios de Derecho de la Sociedad de la Información*. Cizur Menor: Aranzadi.

En el supuesto de que en el tratamiento causante de los perjuicios hayan participado más de un responsable o encargado, cada uno será responsable de la totalidad del daño causado, con el fin de garantizar el pago de la indemnización del interesado. Evidentemente, si en tal caso uno de los responsables paga la totalidad del daño producido, entonces podrá reclamar a los demás la parte

[14] *A contrario sensu*, cuando una Administración pública no actúe en ejercicio de sus poderes públicos, el interesado podrá ejercer la acción de responsabilidad en el Estado miembro donde tenga el domicilio (Nieto, 2016, págs. 565).

de daños que les corresponda. Serán competentes para resolver estas acciones de indemnización los tribunales donde el interesado tenga su residencia habitual, a menos que sea una Administración pública en ejercicio de poderes públicos[14]. Finalmente, cuando el responsable sea una Administración pública española, la responsabilidad será objetiva, y el interesado podrá reclamar responsabilidad patrimonial frente a la Administración, aunque no haya dolo, culpa o negligencia[15]. Por consiguiente, si la actuación administrativa es la causa del daño, y este es evaluable, deberán indemnizarse los daños causados[16].

(15)De acuerdo con el art. 106.2 CE, arts. 32-34 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público. La Administración no podrá repetir contra su personal si este no incurrió en dolo, culpa o negligencia (art. 36 de la misma Ley).

(16)A diferencia del régimen de responsabilidad del art. 1902 del Código civil, en el cual es preciso demostrar la existencia de dolo o negligencia en la acción que causa el daño.

3) Régimen sancionador económico o multas administrativas en el RGPD

Las autoridades de control podrán imponer multas administrativas –es decir, sanciones económicas– por infracciones del RGPD, efectivas, proporcionadas y disuasorias (art. 83 RGPD)[17] (Corral, 2016). El objetivo del régimen sancionador del RGPD consiste en armonizar la actual disparidad de niveles de sanción en los estados miembros[18]. Por ello, la regulación es muy detallada y no se deja margen a los estados. Se amplían, por ejemplo, los sujetos pasivos, que no se limitan a los responsables y encargados (cosa que sí hacía, en cambio, el art. 43 LOPD). Junto con estos, el RGPD prevé también sanciones para los organismos de certificación y los organismos de supervisión de los códigos de conducta[19].

(17)En los estados en los cuales la imposición de multas económicas se reserve a los tribunales, la autoridad de control incoará el procedimiento y serán los tribunales quienes impongan la sanción (art. 89.3 RGPD).

(18)El art. 24 de la Directiva 95/46/CE dejaba un amplio margen a los estados a la hora de fijar las sanciones, y las diferencias eran notables en la práctica (considerandos 148 y 150 del RGPD). Se busca, así, evitar los «paraísos de datos» en la Unión Europea.

(19)Art. 83.4 RGPD, en relación con los arts. 42 y 43, y 41.4 RGPD. Esto es coherente con las responsabilidades que les atribuye el RGPD. En la versión en español del RGPD, el art. 83.4c contempla aparentemente sanciones administrativas a las autoridades de control, cuando en la versión en inglés se refiere a *monitoring body* y no, en cambio, a *supervisory authorities*.

Lectura recomendada

A. Corral (2016). «El régimen sancionador en materia de protección de datos en el Reglamento General de la Unión Europea». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 571-585). Madrid: Ed. Reus.

Pues bien, las multas administrativas serán adicionales o sustitutivas de las medidas del art. 58.2a-h y j RGPD. Esto significa que la comisión de una infracción no supone necesariamente la imposición de una multa: la multa puede ser adicional, pero se puede sustituir por otras medidas correctivas. Por consiguiente, primero será necesario analizar si se impone multa u otra medida, a partir de los hechos del caso; y cuando se opte por la multa, deberá valorarse su cuantía según las circunstancias del caso[20]. Pese a todo, no se trata de un régimen completo, pues se deja en determinados aspectos un margen a los estados. En lo que quede fuera del ámbito de aplicación material del RGPD, y cuando este deje un margen de apreciación a los estados –sanciones no económicas, como veremos–, la LOPD, o la norma que la sustituya, podrá incorporar un régimen sancionador adicional (Corral, 2016, págs. 572-573).

(20)Hay un margen de apreciación amplio, pero se trata de potestades regladas. Se trata de un abanico demasiado amplio, de 0 a 10 millones de euros.

Veamos ahora el régimen sancionador económico del RGPD. La multa se impondrá teniendo en cuenta los siguientes aspectos (art. 83.2 RGPD):

- La gravedad de la infracción, según el tipo de tratamiento, el número de interesados afectados y los daños y perjuicios sufridos.
- La intencionalidad o, por el contrario, la negligencia en la infracción.
- Las medidas tomadas para paliar los daños.
- El historial anterior de infracciones del responsable o encargado: este aspecto es importante, pues permite decidir si iniciar uno o varios procedimientos contra el mismo responsable. Por ejemplo, la Information Commissioner's Oficce (ICO) del Reino Unido decidió, en un contexto en el cual tenía cuatro incidentes contra el mismo responsable, sancionar solo por el más grave y, en los demás, llevar a cabo una simple advertencia informal (Grant y Crowther, 2016, pág. 295).
- La cooperación con la autoridad de control: quizá también pueda considerarse aquí el pronto pago de las multas, con un descuento sobre el importe total.
- Las categorías de datos afectadas.
- Si hubo notificación de la infracción.
- La adhesión a códigos de conducta.
- Los posibles beneficios económicos derivados de la infracción.

No se contempla, en cambio, en el RGPD el criterio usado por algunas autoridades de control de valorar el nivel económico del responsable a la hora de modular la multa impuesta[21]. Con todo, de acuerdo al considerando 148 del RGPD, si la aplicación de una sanción fuera valorada como desproporcionada, se podría optar entonces por otras medidas. De hecho, es habitual que esta valoración del nivel económico no se prevea expresamente en ningún precepto, sino que derive del margen de discrecionalidad de las autoridades de control. Quizá la misma práctica acabará imponiéndose también en la aplicación del RGPD. En el caso de incumplimiento de varias obligaciones previstas en el RGPD, se establece un límite máximo para la multa administrativa consistente en las infracciones más graves.

[21]En mayo del 2011, la ICO redujo de 200.000 a 1.000 libras esterlinas la multa al responsable Andrew Crossley de ACS Law, con recursos económicos limitados. En cambio, la multa a Sony Computer Entertainment de enero del 2013 no se vio reducida.

En todo caso, se prevén unas multas administrativas de 10 millones de euros como máximo, o el 2 % de su volumen de negocio anual del ejercicio financiero anterior, la que resulte mayor, en los siguientes casos[22] (art. 83.4 RGPD):

[22]No se sigue un modelo de tres escalas, como en el LOPD.

- Obligaciones del responsable o encargado contenidas en los arts. 8, 11, 25 a 39, 42 y 43 RGPD: es decir, en supuestos de vulneración de las normas sobre consentimiento de menores; tratamientos que no requieren teóricamente identificación; protección de datos desde el diseño y por defecto; responsabilidades del encargado; seguridad de los datos; evaluación de impacto relativa a la protección de datos; consulta previa; delegado de protección de datos; y certificación.

- Obligaciones de los organismos de certificación (arts. 42 y 43 RGPD).

- Obligaciones del órgano supervisor de códigos de conducta en caso de infracción del código por el responsable o encargado (art. 41,4 RGPD).

Las multas administrativas podrán incluso llegar a los 20 millones de euros como máximo o, en el caso de una empresa, con el 4 % de su volumen de negocio anual del ejercicio financiero anterior, la que resulte una cantidad mayor[23]. Puede parecer una cantidad muy exagerada, pero hay que tener en cuenta que la Federal Trade Comission (FTC) americana ya impuso multas de 32,5 millones y 22,5 millones de dólares a Apple y Google en el 2013 y el 2014. Y en estos casos, las multas no eran lo peor para estos gigantes, sino la publicidad negativa asociada a los procedimientos sancionadores, por su efecto sobre la confianza de los consumidores en estas empresas. El RGPD ha supuesto, en este sentido, un cambio notable en relación con las multas pre-RGPD, calificadas en ocasiones gráficamente como *pocket-money* o calderilla, si tenemos en cuenta los volúmenes de negocio de algunos gigantes de Internet (Reding, 2014). De manera comparativa, las multas por infringir las reglas de la competencia o en materia financiera son significativamente más onerosas: decenas o hasta centenares de millones de euros[24]. En definitiva, se trata de intentar evitar que sea más barato y beneficioso para el responsable del tratamiento incumplir la normativa y pagar una multa que cumplir con la legislación vigente.

[23]Existen dudas de que el principio de tipicidad no se vea comprometido con preceptos como el 83.4 y el 83.5 RGPD: primero, por la remisión a todo un artículo, con la indeterminación que esto supone; pero sobre todo, por tener asociadas sanciones de 0 a 20 millones o el 4 % del volumen de negocio global de una empresa. Este margen de apreciación puede resultar incompatible con el principio de tipicidad, y generar inseguridad jurídica (Corral, 2016, pág. 579).

[24]Puede verse, por ejemplo, la multa de 163 millones de libras esterlinas al Deutsche Bank impuesta por la Financial Conduct Authority (FCA) británica en enero del 2017. Para más información, podéis ver: «FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings»

Los incumplimientos contemplados en este caso son (art. 83.5 RGPD):

- Principios básicos para el tratamiento de los datos, licitud del tratamiento, condiciones para el consentimiento y tratamientos de categorías especiales de datos (arts. 5, 6, 7 y 9 RGPD).

- Derechos de los interesados (arts. 12 a 22 RGPD).

- Transferencias de los datos personales a un destinatario en un tercer país o una organización internacional (arts. 44-49 RGPD).

- De acuerdo con el Derecho español, conciliación con la libertad de expresión; documentos oficiales; DNI; tratamiento en el ámbito laboral; archivo en interés público o con fines de investigación científica o histórica, o

fines estadísticos; obligaciones de secreto y datos de las iglesias; y asociaciones religiosas (arts. 85-91 RGPD).

- Incumplimiento de resoluciones, limitaciones temporales o definitivas de tratamiento, suspensión de los flujos de datos decidida por una autoridad de control (58.2 RGPD), o no facilitar el acceso a la misma (art. 58.1 RGPD).

Cada Estado miembro decidirá si en este caso se pueden imponer multas administrativas a autoridades y organismos públicos (art. 83.7 RGPD). La imposición de estas multas administrativas estará sujeta a tutela judicial efectiva y a un proceso con todas las garantías procesales debidas. Pese a que el RGPD parece mostrar mucha confianza en la eficacia de las sanciones monetarias, los resultados anteriores a este texto no son nada halagüeños[25]. Si nos atenemos a la cantidad de datos efectivamente tratados, la imposición de sanciones es un escenario relativamente excepcional. Normalmente, las sanciones se reservan para los casos más graves y tradicionales, los de violación de seguridad, y en muchos casos, frente a responsables del sector público[26]. Los procedimientos de cooperación y las auditorías consensuadas son mucho más frecuentes. También es habitual el fomento de la formación del personal que debe tratar los datos personales, las guías y códigos de buenas prácticas y el fomento general de las prácticas de buen gobierno en la Administración.

(25)Por ejemplo, entre abril y diciembre del 2013, la Information Commissioner's Office (ICO) del Reino Unido informó sobre 1.152 incidentes de violación de la seguridad de los datos, mientras que solo se impusieron 15 sanciones monetarias en el mismo periodo. Para más detalles, podéis ver Grant y Crowther (2016, págs. 287-305).

(26)Entre el 2010 y junio del 2014, tan solo 64 sanciones monetarias fueron impuestas por la ICO del Reino Unido, aunque algunas por sumas considerables, de hasta 325.000 libras esterlinas, contra los hospitales universitarios de Brighton y Sussex NHS Trust, en junio del 2012 (Grant y Crowther, 2016, págs. 288 y 297).

La idea que subyace a la imposición de multas administrativas es la de disuadir al responsable que ha sido multado de continuar infringiendo el RGPD. Se espera, así, que el responsable que ha sido multado rectifique el motivo que le ha llevado al incumplimiento, ya sea mediante mejoras procedimentales, cambiando los tratamientos de datos o bien añadiendo los controles debidos. De hecho, puesto que se ha recibido anteriormente una sanción por incumplimiento, la percepción de la protección de datos pasa a ser ya no un mero riesgo legal, sino un auténtico riesgo corporativo que hay que afrontar con una buena gestión de la información. Ahora bien, el efecto disuasorio no opera únicamente frente a las empresas sancionadas en el pasado sino, de manera más general, frente a todos los demás responsables. Una campaña mediática por parte de la autoridad de control suele hacer más efectiva esta disuasión. Otra muestra de este buscado efecto mediático es que no suele haber multas bajas, por ejemplo, por debajo de 40.000 libras esterlinas, en el caso de la ICO británica (Grant y Crowther, 2016, pág. 297). De hecho, en algún caso, la importancia social de la infracción ha jugado en contra del responsable, como en el envío no solicitado de textos de marketing directo[27].

(27)El caso Tetrus Telecoms en el Reino Unido, en noviembre del 2012.

El perfil del delegado de protección de datos (DPO, en inglés) se ha visto también reforzado por las sanciones, y cobra importancia su tarea de protección de los datos personales en el proceso de decisión corporativo. El análisis de cos-

tes/beneficios puede cambiar totalmente después de una sanción de 325.000 libras esterlinas, y la inversión en encriptación no parece entonces un gasto inútil y elevado, sino una inversión para evitar un riesgo grave para la empresa. Además, considerar el aviso a la autoridad de control como un atenuante en la imposición de las sanciones tiene un efecto de incentivo no desdeñable sobre los responsables que detectan violaciones de seguridad. Las cuantías de 20 millones de euros en el RGPD parecen un claro mensaje a los responsables internacionales que tratan cantidades ingentes de datos. No se prevé en el RGPD la posibilidad de indemnizar a los interesados con las multas cobradas, ni destinar los ingresos al fomento de la protección de datos.

Tampoco parece que antes del RGPD se haya tenido en cuenta, al menos en el nivel que parece contemplarlo la autoridad de control del Reino Unido, el criterio del beneficio económico que el responsable haya obtenido con la infracción, a la hora de fijar la cantidad de la multa. De hecho, en los casos multados de violación de la seguridad de los datos, el responsable no obtiene beneficio económico alguno con la infracción[28]. Por ello, se ha sugerido como alternativa para un supuesto de violación de seguridad de los datos que se imponga el gasto de adoptar las medidas para cumplir con el RGPD, en lugar de multar. En todo caso, si las multas se ciñen de manera preferente sobre las violaciones de seguridad, esto provocará rechazo, pues en no pocas ocasiones la violación se debe a una actuación de un tercero[29]. Se sanciona en estos casos al responsable por no haber sido capaz de proteger la información debidamente. Es más fácil de aceptar por parte del responsable su responsabilidad en los casos de actuación indebida, como *spam* o marketing directo no solicitado.

(28)El RGPD sí menciona, en cambio, el beneficio económico como un agravante (art. 83.2k RGPD).

(29)Siguiendo con la ICO inglesa, al Croydon Council se le impuso una multa de 100.000 libras esterlinas en febrero del 2012, después de que un bolso de una empleada fuera robado; a Sony también se le impuso una multa de 250.000 libras esterlinas, después de un acceso no autorizado mediante un método sofisticado, en enero del 2013; y al Glasgow City Council se le impuso otra multa de 150.000 libras esterlinas en junio del 2013, después del robo de dos portátiles no encriptados de sus oficinas.

Las multas suelen recurrirse, cosa que no sucede con las medidas alternativas que veremos a continuación, lo cual supone un gasto añadido también para la autoridad de control. Otro aspecto que hay que tener en cuenta cuando se centra demasiado la respuesta en las multas es que el efecto de publicidad decae con el tiempo, y la cobertura mediática a las primeras multas ya no se mantiene en el futuro si estas se generalizan. Eso sí, la primera multa de 20 millones impuesta por una autoridad de control en cumplimiento del RGDP será noticia, con toda seguridad. Muchas veces, una auditoría consigue más cambios en la empresa que una multa. E incluso en el caso de violaciones de seguridad, la empresa tiende a adoptar medidas correctoras para evitar que su reputación se vea comprometida en el futuro, más que temiendo una multa o debido a la imposición de una multa. También se plantea la idoneidad de multar a administraciones públicas, cuando en este caso no se dispone de los recursos y no hay el incentivo de reducir los beneficios, puesto que no se obtienen beneficios.

4. Régimen sancionador nacional

En los supuestos no contemplados como sancionables mediante multas administrativas por el art. 83, apartados 4, 5 y 6 RGPD, el Estado miembro preverá sanciones que, al igual que sucede con las multas administrativas, serán proporcionadas y disuasorias para las infracciones del Reglamento y las medidas para su aplicación efectiva (art. 84 RGPD). Aquí, el margen para la legislación nacional es mayor[30]. Estas disposiciones legislativas serán comunicadas a la Comisión, así como cualquier reforma posterior de las mismas. España ha tenido en los últimos veinticinco años el régimen sancionador europeo más severo por infracciones de la normativa de protección de datos (Rallo, 2016).

[30]El amplio margen a los estados parece más propio de una Directiva que de un Reglamento, y contrasta con el art. 83 RGPD.

Lecturas recomendadas

Sobre el régimen sancionador español, podéis ver los siguientes trabajos:

A. Rallo (2016). «The Spanish Experience of Enforcing Privacy Norms: two Decades of Evolution from Sticks to Carrots». En: D. Wright; P. de Hert (eds.). *Enforcing Privacy. Regulatory, Legal and Technological Approaches* (págs. 123-144). Berlín: Springer.

I. Gómez-Juárez (2008). «Estudio del régimen sancionador de la LOPD». *Revista Española de Protección de Datos* (núm. 4, enero-junio, págs. 159-173).

Esto fue posible ya desde la LORTAD de 1992, y se prolongó sin demasiados cambios, tras la LOPD, hasta la actualidad[31]. El título VIII del APLOPD prevé el régimen sancionador, y para ello retoma la regulación del RGPD y la completa. En cuanto a los sujetos responsables, destaca la exclusión de los delegados de protección de datos a los que no se les aplica este régimen sancionador (art. 70.2 APLOPD).

[31]Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Fue derogada por la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

Dentro del margen de maniobra que deja el RGPD, el legislador español, por el momento, ha decidido no establecer sanciones económicas para las administraciones públicas. Pese a que el art. 83 RGPD establece dos niveles de sanciones, el APLOPD ha previsto en cambio tres niveles:

- Infracciones muy graves.
- Infracciones graves.
- Infracciones leves.

Las **infracciones muy graves** (art. 72 APLOPD) serán las contenidas en el art. 83.5 RGPD y prescribirán a los 3 años. Se destacan del art. 83.5 RGPD las siguientes infracciones muy graves:

- Vulneración de los arts. 5, 6 y 7 RGPD.

- Utilización de los datos para otra finalidad incompatible con aquella para la que fueron recopilados, sin el consentimiento del afectado y sin base legal para ello.

- Tratamiento de datos de las categorías del art. 9 RGPD sin que concurran las circunstancias previstas en este precepto ni en el art. 10 RGPD.

- Tratamiento de datos de condenas e infracciones penales o medidas de seguridad fuera de los supuestos permitidos en el art. 10 RGPD y art. 20 APLOPD.

- Tratamiento de datos de carácter personal relacionados con infracciones administrativas fuera de los supuestos del art. 4 APLOPD.

- Omisión del deber de informar al afectado (arts. 13 y 14 RGPD) o exigencia del pago de un canon para ser informado o para ejercer los derechos de los arts. 15 a 22 RGPD. De igual manera, la obstaculización o no atención reiterada al ejercicio de estos derechos de los arts. 15 a 22 RGPD.

- Vulneración del deber de confidencialidad (art. 6 APLOPD).

- Transferencia internacional de datos personales sin las garantías de los arts. 44 a 49 RGPD.

- Incumplimiento de las resoluciones de la AEPD o autoridad autonómica de protección de datos competente (art. 58.2 RGPD).

- Incumplimiento de la obligación de bloqueo.

- No facilitar el acceso u obstaculizar el ejercicio de la investigación o inspección por parte del personal de la AEPD u otra autoridad autonómica de protección de datos competente.

En cuanto a las **infracciones graves**, que prescriben a los 2 años, el art. 73 APLOPD destaca los siguientes supuestos del contenido del art. 83.4 RGPD:

- Tratamiento de datos personales de un menor de 13 años sin el consentimiento del titular de la patria potestad o tutor –no así del menor, pues este no puede consentir válidamente si es menor de 13 años de acuerdo al art. 8.1 APLOPD–, o no acreditar un esfuerzo razonable para verificar la validez del mismo.

- Impedir, obstaculizar o no atender a los derechos de acceso, rectificación, supresión, limitación o portabilidad cuando, sin requerirse la identificación del usuario, este haya facilitado su identificación.

- Falta de medidas técnicas en aplicación del principio de protección de datos por el diseño o por defecto (art. 25,1 RGPD) y para garantizar que solo se tratarán los datos necesarios para la finalidad concreta (art. 25.2 RGPD).

- Falta de designación de un representante del responsable o encargado no establecido en la Unión Europea (art. 27 RGPD), o falta de atención del representante a la AEPD o equivalente autonómico.

- Contratación de un encargado que no ofrezca las garantías necesarias o encargar a un tercero el tratamiento sin ningún contrato o sin contar con la autorización del responsable (art. 28.3 RGPD).

- Infracción por parte del encargado del RGPD y del APLOPD en cuanto a los fines y medios del tratamiento, o no notificar al responsable o a la autoridad de control las violaciones de seguridad detectadas.

- Falta de registro de tratamiento de datos o no ponerlo a disposición de la AEPD o autoridad autonómica equivalente, cuando esta lo solicite.

- No cooperar con las autoridades de control, ni haber efectuado la consulta previa cuando esta sea exigible (art. 36 RGPD).

- No hacer una previa valoración de los riesgos, ni una evaluación del impacto cuando sea exigible (art. 30 RGPD).

- No comunicación al afectado de una violación de seguridad cuando lo requiere la AEPD.

- No designación de delegado de protección de datos cuando sea exigible (art. 37 RGPD) o impedir el ejercicio de sus funciones.

- Uso de sello o certificación de entidad no acreditada o cuya vigencia haya expirado.

- Obtener acreditación presentando información inexacta (art. 43 RGPD).

- Actuar como un organismo de certificación o como un organismo de supervisión de un código de conducta, sin estar acreditado (arts. 40 y 41 RGPD, respectivamente); o, en el primer caso, incumpliendo los principios y deberes de los arts. 42 y 43 RGPD; o en el segundo, sin adoptar medidas en caso de infracción de un código.

Las **infracciones leves**, que prescribirán al año, serán incumplimientos meramente formales de las previsiones del art. 83, 4 y 5. El art. 74 APLOPD concreta los siguientes supuestos:

- Incumplimiento del principio de transparencia y derecho a información o la exigencia del pago de un canon para facilitar la información (arts. 13 y 14 RGPD).

- No atender ocasionalmente la solicitud de ejercicio de los derechos de los arts. 15 a 22 RGPD.

- Incumplimiento de la obligación de notificación sobre la rectificación, la supresión o la limitación del tratamiento (art. 19 RGPD) o de la información a los afectados de los destinatarios a los que se han comunicado estos datos.

- Incumplimiento de la obligación de suprimir los datos de las personas fallecidas cuando fuera exigible (art. 3 APLOPD).

- Falta de formalización de las responsabilidades de cada corresponsable, o no poner el acuerdo a disposición de los afectados.

- Falta de información al responsable sobre la infracción del RGPD de una instrucción suya al encargado (art. 28.3 RGPD).

- Incumplimiento del contrato o de las instrucciones del responsable por parte del encargado, excepto si es para no infringir el RGPD.

- Disponer de un registro de tratamiento incompleto (art. 30 RGPD).

- Informar de manera incompleta de una violación de seguridad a la AEPD o autoridad autonómica, o no documentarla (art. 33 RGPD).

- No comunicar al afectado una violación de seguridad.

- Facilitar información inexacta a la AEPD en el supuesto de una comunicación previa (art. 36 RGPD).

- No publicar o no comunicar a la AEPD o autoridad autonómica los datos de contacto del delegado cuando sea necesario su nombramiento (art. 37 EGPD).

- No informar, por parte de un organismo de certificación o por parte de un organismo acreditado de supervisión de códigos de conducta, a la AEPD o autoridad autonómica de la expedición, renovación o retirada de una certificación o bien de las medidas oportunas en caso de infracción del código (art. 41.4 RGOD).

Las sanciones previstas en el art. 83, apartados 4, 5 y 6 RGPD se aplicarán teniendo en cuenta los criterios de graduación que ya hemos visto con anterioridad (art. 83.2 RGPD). El art. 76.2 APLOPD completa estos criterios con nuevos aspectos que hay que tener en cuenta:

- El carácter continuado de la infracción.

- La posibilidad de que la conducta del afectado hubiera inducido a la comisión de la infracción.

- La fusión por absorción posterior a la comisión de la infracción no imputable a la entidad absorbente.

El legislador nacional deja abierta la posibilidad, complementaria o alternativa, de imponer las restantes medidas correctivas contenidas en el art. 83.2 RGPD. Se prevé, asimismo, la publicación en el BOE de la identidad del infractor, de la infracción cometida y del importe de la sanción cuando se trate de la AEPD, para una sanción superior a un millón de euros y cuando el infractor sea una persona jurídica (art. 76.4 APLOPD).

Se prevé un régimen especial para ciertas categorías de responsables o encargados de órganos constitucionales, administrativos, corporaciones de derecho público y universidades públicas (art. 77 APLOPD). Las infracciones muy graves, graves y leves cometidas por estos responsables y encargados acarrearán una resolución de apercibimiento. En la misma, se especificarán las medidas correctoras. Se comunicarán al responsable o encargado, al órgano superior jerárquico y, en su caso, a los afectados que sean interesados. La AEPD o autoridad autonómica podrá iniciar actuaciones disciplinarias de acuerdo al régimen disciplinario o sancionador aplicable. Se informará al defensor del pueblo, u órgano equivalente autonómico, sobre las actuaciones efectuadas y las resoluciones dictadas. La AEPD publicará en su página web, en un lugar previsto al efecto, la sanción impuesta y la identidad del responsable o encargado que haya cometido la infracción.

5. Medidas alternativas o complementarias

Las autoridades de control están introduciendo cada vez más medidas complementarias a las sanciones[32]. La razón es, simplemente, mejorar la aplicación de la legislación de protección de datos. Es decir, existe el riesgo de que algunos responsables consideren las sanciones como el «billete del aparcamiento», que pagan sin alterar sus procedimientos ni medidas de seguridad. También puede darse el caso de sanciones impuestas sin ofrecer ninguna guía de cómo podrían evitarse y mejorar en el cumplimiento de la protección de datos.

(32)Una lista de las posibles medidas de aplicación del RGPD que podrían adoptar las autoridades de control nacionales, más allá de la imposición de multas, puede verse en Wright (2016).

Por estas razones, se ha extendido la práctica de trasladar avisos por escrito antes de llegar a imponer una multa. Por ejemplo, la ICO británica envió un aviso escrito o *enforcement notice* al Ayuntamiento de Glasgow el 4 de junio del 2013, para avisarle de que creara otro registro de entradas de datos. La misma autoridad de control exigió el nombramiento de un responsable de datos, un programa de formación y la encriptación de los ordenadores móviles a los responsables policiales de Derbyshire, el 18 de junio del 2013. Evidentemente, si el responsable no cumple con el aviso escrito, se expone entonces a una multa[33]. La posibilidad de recurso ante los tribunales frente a la multa gana entonces en claridad, pues la infracción es más fácil de probar objetivamente. La reforma española de la LOPD del 2011 también introdujo este mecanismo reactivo en caso de violación de seguridad de los datos (art. 45.6 LOPD):

(33)Quizá esto sea lo que acabe incorporándose en el incumplimiento de los derechos que, de acuerdo con el art. 83 RGPD, debería llevar a una sanción grave.

- Se permite la discrecionalidad de la AEPD a la hora de imponer, o no, una multa en algunas circunstancias.

- La advertencia por escrito no es una sanción, pero no por ello se adopta automáticamente cuando se presenta una demanda.

- Se valorarán primero los hechos y los criterios significativos de la modulación y la degradación contenidos en la LOPD: por ejemplo, no se darán advertencias en casos sin reducción de responsabilidad o ilegalidad en redes sociales, Internet o recopilación de datos en Internet; tampoco si están afectados datos sensibles por violación de seguridad de los datos mediante Internet; o, finalmente, cuando el infractor procesó un volumen muy elevado de datos.

- Solo es aplicable para una primera infracción, y no se permite si el responsable ya ha sido previamente multado o advertido, incluso por hechos distintos de los presentes.

- No se aplica a las infracciones muy graves.

- Si la advertencia es desoída, entonces el procedimiento sancionador empieza.

Otra alternativa a las multas ha consistido en medidas colaboradoras con el responsable, o iniciativas. Así, en el 2014, la ICO llevó a cabo más de 40 iniciativas de colaboración con responsables, por solo 11 multas impuestas y 10 avisos por escrito en el mismo periodo (Grant y Crowther, 2016, pág. 299). En algunas ocasiones, las medidas se adoptan conjuntamente, pues el inicio del procedimiento sancionador impulsa la colaboración. La estrategia parece consistir en usar los avisos o las iniciativas de colaboración cuando la autoridad de control no tiene confianza suficiente en que la multa, por sí sola, sea un remedio efectivo, ni siquiera con el impacto público asociado normalmente a la multa, y mucho menos en el caso de los avisos escritos y las iniciativas de colaboración.

El art. 58.2 RGPD atribuye poderes correctivos a las autoridades de control:

- Sanciones consistentes en una advertencia o en un apercibimiento, según se pueda infringir o se haya infringido el RGPD.

- Órdenes al responsable o al encargado para que atiendan las solicitudes de ejercicio de derechos o comuniquen violaciones de seguridad de los datos personales.

- Imponiendo limitaciones temporales o definitivas.

- Retirando certificaciones.

- Ordenando la suspensión del flujo de datos.

Conviene resaltar finalmente la referencia que el art. 58.2.i RGPD hace al art. 83 RGPD[34], en la cual las multas administrativas parecen contemplarse «además o en lugar de las medidas mencionadas en el presente apartado».

(34)Para ampliar sobre el contenido del art. 58.2 RGPD y sobre su articulación con el art. 83 RGPD, puede consultarse la ponencia de Carles San José en el Ciclo de conferencias sobre el RGPD, organizado por la APDCAT. Podéis ver la sesión del 9 de marzo de dicho ciclo en: «Cicle RGPD, 5a. Jornada. Garanties per a una protecció efectiva del dret a la protecció de dades».

En definitiva, el RGPD parece optar claramente por un sistema de aplicación del Reglamento basado en multas administrativas impuestas por las autoridades de control. Estas juegan múltiples roles simultáneamente: guía, policía, fiscal y juez (De Hert y Boulet, 2016). Esta preferencia por la aplicación administrativa es coherente con la condición de última ratio del Derecho penal, pero no debe menoscabar principios legales elementales como la tutela judicial efectiva y el derecho al proceso debido. La acumulación de roles de policía y fiscal, así como la creciente discrecionalidad a la hora de decidir imponer o no una multa, plantean no pocas cuestiones en un contexto de multas eleva-

(35)Este modelo existe ya en el ámbito de la protección del medio ambiente.

das, como impone el RGPD. La última ratio penal no puede, de este modo, servir como excusa para transformar el Derecho administrativo en un Derecho cuasipenal sin garantías, o con muchas menos garantías que las reservadas al Derecho penal (De Hert y Boulet, 2016, págs. 387-388). En el RGPD, la aplicación mediante multas administrativas es obligatoria, mientras que la posible protección por medio de ilícitos penales es opcional. La falta de armonización penal plantea, así, problemas, pues podría haberse optado por excluir el Derecho penal directamente: la simple posibilidad de imposición de penas por infracción de la protección de datos crea ahora un régimen potencialmente fragmentado. Quizá se podría pensar en un modelo de «cohabitación» entre Reglamento y Directiva, con una Directiva para armonizar los aspectos relativos a la protección de datos mediante el Derecho penal[35] (De Hert y Boulet, 2016, pág. 389).

Ejercicios de autoevaluación

Estos ejercicios de autoevaluación son generales, hacen referencia a los seis módulos de la asignatura.

1. Una empresa recoge datos personales de sus empleados para gestionar salarios y seguros de enfermedad, entre otros fines. La legislación obliga a la empresa a enviar los datos de salarios al Ministerio de Hacienda, para reforzar el control fiscal. ¿Se trata de un supuesto de corresponsabilidad?

2. La empresa Publi, S. A. contrata a distintas organizaciones para efectuar campañas de publicidad por correo electrónico. Da instrucciones precisas sobre la publicidad que debe enviarse, a quién, cómo pagar, qué cantidades y en qué fechas. Las organizaciones deciden el software que hay que usar. Publi, S. A. asesora en caso de dudas, y solo ella tiene derecho a usar los datos procesados. A la vista de estos datos, ¿debe considerarse a Publi, S. A. responsable o encargada de los datos?

3. La empresa Marketing, S. A. presta servicios de publicidad y marketing a varias empresas. Comercial, S. A. firma un contrato con Marketing, S. A. para que esta última lleve a cabo publicidad para los clientes de la primera. Marketing, S. A. es considerada encargada del tratamiento de datos. Marketing, S. A. decide utilizar la base de datos de Comercial, S. A. también para promocionar los productos de otros clientes. ¿Marketing, S. A. es encargada o responsable?

4. Un miembro de la dirección de Vigilan, S. A. decide vigilar en secreto a los empleados de la empresa, a pesar de que esta decisión no cuenta con el respaldo formal de ningún acuerdo de la dirección. ¿Quién es, en este caso, el responsable del tratamiento de los datos?

5. Un propietario de un inmueble firma un contrato con Seguri, S. A. para instalar unas cámaras de vigilancia en distintos puntos del inmueble. Los fines, y cómo se recogen y almacenan las imágenes, es algo que determina el propietario. ¿Es el propietario el único responsable del tratamiento, o Seguri, S. A. es corresponsable?

6. Viaje, S. A. envía datos personales a la compañía aérea Vuele, S. A. y a una cadena hotelera, Hotel, S. A., para hacer las reservas de los paquetes de viaje. La compañía aérea y el hotel confirman la disponibilidad de las plazas. Viaje, S. A. emite los documentos de viaje para sus clientes. ¿Viaje, S. A., Vuele, S. A. y Hotel, S. A. son corresponsables, o responsables por separado?

7. Viaje, S. A., Vuele, S. A. y Hotel, S. A. deciden crear una plataforma común en Internet para mejorar su gestión de las reservas de viajes. Acuerdan los medios que hay que usar, como el tipo de datos que se almacenarán, la forma y la confirmación de las reservas y quién podrá acceder a la información. Comparten los datos para hacer marketing común. ¿Son, por ello, corresponsables del tratamiento?

8. Los proveedores de servicios de redes sociales –correo electrónico o acceso a Internet– ponen a disposición de los usuarios plataformas de comunicación que les permiten publicar e intercambiar información. ¿El proveedor es responsable, o son responsables o corresponsables también los usuarios? ¿Y si se trata de un proveedor de servicios que aloja datos en Internet?

9. Varios bancos pueden decidir crear una base de datos de morosos en la que cada uno introduce información sobre clientes morosos, y a la que todos tienen acceso. Puede que se haya designado a un proveedor o punto de acceso. ¿Cómo se localiza entonces al responsable para poder ejercer un derecho?

10. Un sitio web de objetos perdidos en el que las personas publican un anuncio de un objeto perdido, ¿es un encargado del tratamiento?

Solucionario

Ejercicios de autoevaluación

1. Pese a que la empresa y las autoridades fiscales tratan los mismos datos de los salarios, faltan los fines o medios compartidos. Por consiguiente, se trata de dos responsables del tratamiento de datos independientes.

2. Publi, S. A. es responsable del tratamiento de los datos. Cada una de las organizaciones será encargada del tratamiento en lo que respecta a los datos que efectivamente utilice para su actividad de publicidad.

3. Marketing, S. A. es encargada del primer contrato, pero deviene responsable del tratamiento de datos adicional no contemplado en el contrato. Este nuevo tratamiento puede tener, además, un problema de legitimidad, que aquí no nos interesa.

4. Vigilan, S. A. es la responsable del tratamiento, y deberá hacer frente a posibles denuncias de los empleados si hay un uso abusivo de los datos. Esta responsabilidad se debe a que, al ser responsable del tratamiento, debe velar por la seguridad y la confidencialidad adecuadas. Esto no obsta a que la empresa pueda considerar responsable de un uso abusivo al miembro de la dirección en vía civil o penal –por ejemplo, si usa los datos para extorsionar a los empleados. En este caso, el directivo sería responsable del tratamiento por el uso particular de los datos.

5. El propietario es el único responsable, ya que determina los fines y los medios.

6. Cada uno es responsable del tratamiento distinto que lleva a cabo, y sus obligaciones se limitan a los datos tratados en cada caso.

7. En este caso, Viaje, S. A., Vuele, S. A. y Hotel, S. A. tienen un control conjunto sobre cómo se tratan los datos de sus clientes y, por consiguiente, son corresponsables del tratamiento llevado a cabo en la plataforma común de reservas por Internet. Cada uno será, además, responsable de los tratamientos que sean exclusivos, como por ejemplo los datos de cada uno sobre la gestión de recursos humanos.

8. Los proveedores de servicios son responsables del tratamiento de datos, puesto que determinan los fines y los medios. Los usuarios pueden ser responsables si sus actividades no están protegidas por la excepción doméstica (art. 2.2.c RGPD), o uso para fines personales (Dictamen 5/2009 del grupo del artículo 29 sobre las redes sociales en línea, adoptado el 12 de junio del 2009; WP 163). Si se trata, en cambio, de un proveedor de servicios de alojamiento de datos en Internet, entonces se trata de un encargado de datos personales publicados en línea por sus clientes, que lo utilizan para alojar y mantener su sitio web. Sin embargo, si el encargado somete los datos contenidos en los sitios web alojados a un tratamiento adicional para sus propios fines, entonces se convierte en responsable de los datos en relación con ese tratamiento específico.

9. El proveedor o punto de acceso debe ser público, y corresponde a este localizar al responsable del tratamiento competente y velar para que se dé una respuesta adecuada al interesado.

10. Supongamos de entrada que se trata efectivamente de datos personales, pues si solo se mencionan los objetos perdidos, no necesariamente aparece vinculado a un sujeto identificado o identificable. El sitio web se ha creado con una finalidad comercial o de lucro, a partir de la publicación de anuncios de objetos perdidos. El sitio web quizá no determina qué objetos figuran en los anuncios, aunque sí las categorías, pero en todo caso determina las condiciones de la publicación de los mismos. Por tanto, el sitio web de objetos perdidos es responsable del tratamiento de datos.

Bibliografía

AEPD (ed.) (2008). *La potestad sancionadora de la Agencia Española de Protección de Datos*. Cizur Menor: AEPD-Aranzadi.

Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa (2014). *Manual de legislación europea en materia de la protección de datos*. Luxemburgo: Oficina de Publicaciones de la Unión Europea.

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 Protección de Datos*. Valencia: Tirant lo Blanch.

Calvo, E. (2008). «El régimen sancionador de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal». En: AEPD (ed.). *La potestad sancionadora de la Agencia Española de Protección de Datos* (págs. 19-31). Cizur Menor: AEPD-Aranzadi.

Corral, A. (2016). «El régimen sancionador en materia de protección de datos en el Reglamento General de la Unión Europea». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 571-585). Madrid: Ed. Reus.

Gómez-Juárez, I. (2008). «Estudio del régimen sancionador de la LOPD». *Revista Española de Protección de Datos* (núm. 4, enero-junio, págs. 159-173).

Grant, H.; Crowther, H. (2016). «How Effective Are Fines in Enforcing Privacy?». En: D. Wright; P. de Hert (eds.). *Enforcing Privacy. Regulatory, Legal and Tedchnological Approaches*. Berlín: Springer.

Hert, P. de; Boulet, G. (2016). «The Co-existance of Administrative and Criminal Law Approaches to Data Protection Wrongs». En: D. Wright; P. de Hert (eds.). *Enforcing Privacy. Regulatory, Legal and Technological Approaches* (págs. 357-394). Berlín: Springer.

López, J. (2008). «Actividad inspectora y procedimiento administrativo sancionador en materia de protección de datos personales». En: AEPD (ed.). *La potestad sancionadora de la Agencia Española de Protección de Datos* (págs. 253-267) Cizur Menor: AEPD-Aranzadi.

López, L. F. (2016). «La responsabilidad del responsable». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 275-294). Madrid: Ed. Reus.

Nieto, E. (2016). «Derecho a indemnización y responsabilidad». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 555-570). Madrid: Ed. Reus.

Rallo, A. (2016). «The Spanish Experience of Enforcing Privacy Norms: two Decades of Evolution from Sticks to Carrots». En: D. Wright; P. de Hert (eds.). *Enforcing Privacy. Regulatory, Legal and Technological Approaches* (págs. 123-144). Berlín: Springer.

Recio, M. (2016). «Los derechos a presentar reclamaciones ante la autoridad de control y a la tutela judicial efectiva». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 539-553). Madrid: Ed. Reus.

Reding, V. (2014, 19 de enero). «The EU Data protection reform: helping businesses thrive in a digital economy» [documento en línea]. <http://europa.eu/rapid/press-release_SPEECH-14-37_en.htm>.

Vilasau, M.: Vila, M. A. (2010). «Intimidad y datos personales en Internet». En: M. Peguera (coord.). *Principios de Derecho de la Sociedad de la Información*. Cizur Menor: Aranzadi.

Wright, D. (2016). «Enforcing Privacy». En: D. Wright; P. de Hert (eds.). *Enforcing Privacy. Regulatory, Legal and Technological Approaches* (págs. 13-49). Berlín: Springer.