La responsabilidad por incumplimiento de la normativa de datos personales (art. 82 RGPD)

María José Santos Morón[*]

RESUMEN: Cuando una persona sufre daños a consecuencia de un incumplimiento de la normativa de protección de datos tiene la posibilidad de exigir una indemnización. Sin embargo, esta acción de responsabilidad, que está reconocida en el art. 82 RGPD, suscita en España muchas dudas. De entre ellas, en este trabajo se analizan dos cuestiones: la relativa al criterio de imputación de responsabilidad (responsabilidad por culpa u objetiva) y la relativa a la existencia de daño.

PALABRAS CLAVE: Protección de datos; indemnización; responsabilidad por culpa; responsabilidad objetiva; daño.

ZUSAMMENFASSUNG: Wer einen Schaden erleidet, der aus dem Verstoß gegen datenschutzrechtliche Vorschriften resultiert, kann Schadensersatz verlangen. Dieser in Art. 82 DSGVO geregelte Schadensersatzanspruch wirft in Spanien eine Vielzahl von Zweifelfragen auf, von denen zwei Gegenstand des nachfolgenden Beitrages sind: Zum einen die Frage nach Verschuldensabhängigkeit bzw. -unabhängigkeit der Haftung, zum anderen um die Frage nach dem Vorliegen eines Schadens.

SCHLÜSSELWORTER: Datenschutz; Schadensersatz; Verschuldenshaftung; verschuldensunabhängige Haftung; Schaden

* Catedrática de Derecho civil. Universidad Carlos III de Madrid.

1. Planteamiento[1]

La creciente digitalización de la sociedad ha aumentado los riesgos de vulneración de los derechos de la persona, y en particular del derecho a la protección de datos personales. Pensemos que la gran mayoría de las actividades que se realizan en internet (contratación de productos y servicios, descarga de aplicaciones, participación en redes sociales, etc.) conllevan un tratamiento de datos personales. La mera difusión de información atinente a ciertas personas (nombre, dirección, imagen, etc.) en una web de acceso público (ya sea gestionada por un particular[2], un medio de prensa digital, una administración pública, etc.) implica un tratamiento de datos personales. Los operadores de redes sociales son responsables del tratamiento de los datos personales de los usuarios de la red (tanto los que suministran en el momento de la contratación o "alta" en el servicio como de los que comparten a través de la red)[3], al igual que los motores de búsqueda, que

---

1 Este trabajo se ha realizado en el marco del Proyecto PID2020-115352GB-I00, "Daños en el entorno digital: Desafíos en torno a su reparación", financiado por AEI/10.13039/50110001103.

2 Así lo entendió el TJUE en la Sentencia de 6 de noviembre de 2003, caso Linqdvist (C-101-01), en el que la Señora Lindqvist, que ejercía como catequista en su parroquia, creó varias páginas webs para informar a los feligreses de las actividades en ella desarrollada. En dichas páginas incluyó información personal sobre algunos de sus compañeros, y ello fue considerado como un tratamiento de datos que precisaba el consentimiento de los afectados. El TJUE consideró que el tratamiento de datos realizado no encajaba en la excepción relativa a "actividades exclusivamente personales o domésticas" (en cuyo caso no sería aplicable la normativa sobre protección de datos) al resultar los datos publicados en la web accesibles a un número indeterminado de personas.

3 Aunque el considerando 18 del RGDP, incluye la actividad en redes sociales entre los ejemplos cubiertos por la excepción de actividades "personales o domésticas", ello es así en relación con los usuarios (salvo que tengan un perfil abierto accesible a gran número de personas o usen la red con fines comerciales o profesionales). El mismo considerando indica que "no obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas". Los titulares de servicios de redes sociales deben ser considerados como responsables del tratamiento en la medida que deciden sobre la finalidad, contenido y uso del tratamiento de datos que realizan los propios usuarios (cfr. art. 4,7 RGPD). Vid. TRONCOSO, "Redes sociales y protección de datos personales" en *Menores y nuevas tecnologías. Posibilidades y riesgos de la TDT y las redes sociales*, 2013, pp. 91, 92, 94; MEGÍAS QUIRÓS, "Actividades personales y domésticas excluidas del ámbito de aplicación (Comentario al art. 2,2,c RGPD y art. 2,2,a LOPDGDD", en *Comentario al Reglamento General de Protección de Datos y a la Ley orgánica de Protec-*

según la STJUE 13 mayo 2014, Caso *Google Spain* (C-131/12), llevan a cabo un tratamiento de datos personales cuando registran, organizan, conservan y comunican datos personales publicados por un tercero, que aparecen en su lista de resultados.

El que un sujeto, que tiene la consideración de responsable del tratamiento, infrinja la normativa de protección de datos, puede llevar consigo una sanción administrativa[4] que impondrá la autoridad de control -en España la *Agencia Española de Protección de Datos* (AEPD)-, pero el art. 82 del Reglamento General de Protección de datos (Reglamento UE 2016/679) -en adelante RGPD- reconoce también a la víctima la posibilidad de ejercitar una acción de responsabilidad.

Dicho precepto dispone que toda persona que, a consecuencia del incumplimiento de la normativa de protección de datos, haya sufrido un daño material o inmaterial, tiene derecho a obtener una indemnización. En España esta acción de responsabilidad deberá plantearse ante los tribunales civiles cuando el causante del daño sea un sujeto privado –y este es el supuesto que vamos a analizar- y ante la jurisdicción contencioso-administrativa cuando se trate de una institución pública[5].

---

ción de Datos Personales y Garantía de los Derechos Digitales, t. I, Cívitas-Thomson, Cicur-Menor, 2021, pp. 365, 366.

4 Cfr. arts 83, 84 RPGD; arts. 70 y ss. Ley orgánica 3/18, de 5 de diciembre de protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD).

5 Así se deduce del art. 82,6 que se remite a la legislación interna para determinar los tribunales competentes para conocer de esta acción de responsabilidad. Dicho precepto dispone que "las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el art. 79, apartado 2". El citado art. 79,2 permite ejercitar acciones contra el responsable o encargado del tratamiento, bien ante los tribunales del Estado miembro en el que tienen un establecimiento, bien ante los tribunales del Estado miembro en el que el interesado tenga su residencia (con la excepción de que el responsable o encargado sean una autoridad pública de otro Estado miembro y actúen en ejercicio de sus poderes públicos, en cuyo caso el fuero vendrá determinado por el Estado en que radique). Presuponiendo que la víctima del daño ejercite la acción de responsabilidad ante tribunales españoles, deberá dirigirse, como antes se ha indicado, a la jurisdicción civil o contencioso-administrativa, en función de la naturaleza pública o privada del encargado o responsable del tratamiento. LÓPEZ DEL MORAL "Derecho al resarcimiento por los perjuicios derivados de infracciones en materia de protección de datos (Comentario al art. 82 RGPD)" en TRONCOSO, *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, t. II, Cívitas-Thomson, Cicur Menor 2021, p. 3073.

El perjudicado –que debe ser una persona física- puede dirigir la acción, en principio, tanto contra el responsable como el encargado del tratamiento, pero debe tenerse en cuenta que la responsabilidad del encargado del tratamiento es bastante limitada. El párrafo segundo del citado art. 82 indica que el encargado del tratamiento sólo responde de los daños y perjuicios causados por el tratamiento en cuestión cuando "no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable". De ahí que en la mayoría de supuestos en que un tratamiento, que infringe la normativa aplicable, causa daños a un tercero, el sujeto responsable sea el denominado "responsable del tratamiento"[6], que es quien, de acuerdo con el 24 RGPD, que establece el denominado "principio de responsabilidad proactiva", tiene el deber de garantizar que el tratamiento es conforme con el RGPD así como, en su caso, con la normativa interna que concrete o desarrolle el RGPD[7].

En este trabajo nos vamos a centrar en la figura del "responsable del tratamiento", es decir, en los posibles supuestos de ejercicio de una acción indemnizatoria contra el mismo, si bien debe tenerse en cuenta que, conforme al art. 82,4 RGPD cuando en una misma operación e tratamiento intervienen más de un responsable del tratamiento, estos responderán solidariamente.

---

6 El responsable del tratamiento responde frente al titular de los datos personales tanto de los daños derivados de una infracción propia como de los cometidos por su encargado (RUBÍ PUIG, ob. cit., p. 46). Aun en los casos en que pueda existir responsabilidad del encargado (lo que requiere que haya incumplido obligaciones que le son específicamente exigibles, art. 82,2 RGPD) el responsable del tratamiento responderá solidariamente junto con él (art. 82,4 RGPD, art. 30,2 LOPD). Es decir, el responsable del tratamiento no puede liberarse de responsabilidad aduciendo que el comportamiento infractor ha sido cometido por el encargado del tratamiento.

7 Así se deduce del Cdo. 146 RGPD que indica que "un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento". En España, además, el art. 28 LOPD obliga al responsable del tratamiento a garantizar que el mismo es conforme tanto con el RGPD como *con la Ley de protección de datos española y la normativa que la desarrolle.*

La ley española, al igual que sucedía con anterioridad, no ha desarrollado esta acción de responsabilidad[8], lo que suscita ciertas dudas, que voy a abordar en este trabajo.

Del art. 82 RGPD se deduce que, para que pueda exigirse una indemnización al responsable (o, en su caso, encargado) del tratamiento, la víctima debe probar la existencia de:

a) *Una infracción de la normativa de protección de datos*[9].
b) *Un daño*, que puede ser de carácter material o inmaterial.
c) *La relación de causalidad entre la infracción normativa y el daño producido.* Aunque el precepto no lo indica expresamente, esta exigencia debe considerarse implícita dado que es un requisito indispensable en cualquier acción de responsabilidad.

Ahora bien, ¿Es necesario que el responsable del tratamiento -ilícito, incorrecto o no ajustado a la normativa- haya actuado culposa o negligentemente para que pueda condenársele a indemnizar? Dado que el art. 82 RGPD no lo aclara, podría pensarse que ha de llegarse a tal conclusión por aplicación de las reglas generales de responsabilidad (art. 1902 y ss. C.c.). Por otra parte, es necesario que se haya producido algún perjuicio. pero, ¿todo incumplimiento de dicha normativa genera un daño?

El art. 82 suscita muchas otras dudas, relacionadas, por ej. con la articulación de responsabilidad en el supuesto en que existen varios corresponsables del tratamiento o en el supuesto en que el responsable lleva a cabo el tratamiento a través de un encargado. Sin embargo, en este trabajo voy a limitarme a analizar las dos cuestiones señaladas. Esto es, el criterio de imputación de responsabilidad y la existencia de daño.

---

8 En la LORTAD (LO 5/92 de 29 de octubre), el art. 17 se limitaba a disponer que "los afectados, que, como consecuencia del incumplimiento de lo dispuesto en la presente ley por el responsable del fichero, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados". Algo similar ocurría en la LOPD 15/99 cuyo art. 19,1, en aplicación del art. 23 de la Directiva 95/46, establecía que "los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados".

9 Véase lo indicado en la nota 6.

2. Sobre el criterio de imputación de responsabilidad

La doctrina española discute si, para que exista obligación de indemnizar, es preciso que la infracción de la normativa de protección de datos se deba a la culpa o negligencia del responsable (o en su caso, encargado del tratamiento) o si se trata de un supuesto de responsabilidad objetiva, de manera que, existiendo incumplimiento, habrá responsabilidad[10]. Al respecto hay que advertir que, tanto la doctrina como la jurisprudencia española estiman que la responsabilidad no requiere que se haya declarado por parte de la Autoridad de control -en España la AEPD- la existencia de una infracción administrativa merecedora de una sanción. Los tribunales civiles pueden, de manera autónoma, valorar el comportamiento dañoso (art. 42 LEC) y determinar si ha habido incumplimiento normativo[11]. Obviamente, el que un comportamiento concreto esté catalogado como infracción administrativa puede servir como base para concluir que existe un incumplimiento normativo, pero esto no significa

10 En realidad, esta discusión no es nueva, ya que venía planteándose igualmente en relación con el art. 17 LORTAD y con el art. 19 LOPD 15/99. Respecto al precepto de la LORTAD, vid. por todos, GRIMALT SERVERA, pp. 149 y ss., quien, tras exponer las distintas opiniones doctrinales, concluye que la responsabilidad instaurada en dicho texto legal es objetiva. Respecto del art. 19 LOPD puede verse GRIMALT, "Deberes y resonsabilidades en materia de protección de datos", en, CAVANILLLAS MÚGICA, *Deberes y responsabilidades de servidores de acceso y alojamiento (Un análisis multidisciplinar),*Comares, Granada, 2005, p. 200; ABERASTURI GORRIÑO, U. "El derecho a la indemnización en el art. 19 LOPDCP", *Revista Aragonesa de Administración Pública*, 41-42, 2013, p. 190, 191; GARCÍA RUBIO, "Bases de datos y confidencialidad en Internet", en ECHEVARRÍA SÁENZ, *El comercio electrónico,* EDISOFER, Madrid 2001, p. 488; APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 2ª ed., Aranzadi, Cicur-Menor, 2002, p. 167.

11 Vid. PUYOL MONTERO, "Derecho a indemnización", en Troncoso, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Navarra, Thomson-Cívitas, 2010, pp. 1268, 1269; DURÁN CARDO, *La figura del responsable en el derecho a la protección de datos,* Madrid, Wolter Kluwer, pp. 534, 535; BUSTO LAGO, "Protección de datos personales y responsabilidad civil", *Derecho de daños 2020, V Congreso Internacional de Derecho de daños,* 2020, pp. 414, 506 y ss. LÓPEZ DEL MORAL ECHEVERRÍA, "Derecho al resarcimiento por los perjuicios derivados de infracciones en materia de protección de datos (Comentario al art. 82 RGPD)", en TRONCOSO, *Comentario al RGPD y a la LOPDGDD,* T. II, Cívitas-Thomson, Cicur Menor, 2021. En este sentido se pronunció las STS 30 marzo 2011 (RJ 2011/3134). Por su parte, la STS 5 abril 2016 (RJ 2016/1006) afirma que las resoluciones de la jurisdicción administrativa no tienen efecto prejudicial en el proceso civil de indemnización de daños y perjuicios.

que comportamientos no tipificados como infracciones administrativas -o que no encajen totalmente en el tipo legal- no puedan ser tomados en consideración a efectos de imputación de responsabilidad[12].

En cualquier caso, la controversia existente en la doctrina española se debe a que la redacción de los arts. 24 y 82 RGPD genera cierta confusión. Los autores que estiman que el RGPD impone un sistema de responsabilidad por culpa –aunque con inversión de la carga de la prueba- se basan en uno de estos dos argumentos:

a) En primer lugar, el art. 24 RGPD, no solo impone al responsable del tratamiento el deber de garantizar que el tratamiento es conforme con el RGPD, adoptando para ello las medidas técnicas y organizativas adecuadas[13], sino que también le impone la carga de "demostrarlo".

De ahí deduce algún autor que el citado precepto invierte la carga de la prueba de la culpa, de manera que quien reclama una indemnización no tiene que demostrar la culpa del causante del daño, sino que corresponde a éste acreditar que su conducta fue diligente[14].

---

12 Téngase en cuenta que la propia tipificación de infracciones administrativas contenida en los arts. 72 y ss. LOPD, tiene carácter ejemplificativo. Así se indica en la Exposición de Motivos de la LOPD. Ello se explica porque las infracciones vienen determinadas por el RGPD, que considera infracción cualquier incumplimiento del mismo, conteniendo el art. 83 un mero listado de carácter ejemplificativo. Se trata, como observa la doctrina, de una tipificación sumamente "genérica" que parece no adecuarse al principio de tipicidad exigido, en España, en los arts. 25 CE y 27 LRSJP. De ahí que el listado de infracciones contenido en los arts. 72 a 74 LOPD (que distinguen entre infracciones muy graves, graves y leves, aunque sólo a efectos de determinar los plazos de prescripción y no para fijar la cuantía de la sanción) venga dado por la necesidad de cumplir, en la medida de lo posible, el mencionado principio de tipicidad. Vid. GONZÁLEZ ESPADAS, "Infracciones. (Comentario al art. 71 LOPDGDD)", pp. 3095, "Infracciones consideradas muy graves. (Comentario al art. 72 LOPDGDD)", pp. 3116, 3118, "Infracciones consideradas graves. (Comentario al art. 73 LOPDGDD)", pp. 3157, 3158; "Infracciones consideradas leves (Comentario al art. 74 LOPDGDD)", p. 3202, en TRONCOSO, *Comentario al RGPD y a la LOPDGDD,* T. II, Cívitas-Thomson, Cicur Menor, 2021.

13 Vid. DURÁN CARDO, "La responsabilidad del responsable del tratamiento y las obligaciones generales del responsable. El cumplimiento proactivo de la normativa de protección de datos: De la teoría a la práctica (Comentario al art. 24 RGPD y al art. 28 LOPGDD)", en TRONCOSO, *Comentario al RGPD y a la LOPDGDD,* T. II, Cívitas-Thomson, Cicur Menor, 2021, p. 1790.

14 López Álvarez,"La responsabilidad del resposnble", en PIÑAR (dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo de privacidad,* Reus, Madrid, 2016, pp. 280, 281.

Sin embargo, del art. 24 RGP, que instaura el denominado principio de "responsabilidad proactiva" o "accountability"[15], sólo se deduce que corresponde al responsable del tratamiento probar que no ha habido incumplimiento normativo. Es decir, dicho precepto no invierte la carga de la prueba de la "culpa", lo que invierte *es la carga de la prueba de la existencia de una infracción*[16], de modo que, ante la sospecha de que determinado tratamiento infringe algún aspecto de la normativa aplicable, corresponderá al responsable del tratamiento demostrar que no es así[17]. Pero la infracción puede tener lugar sin que se requiera culpa ni negligencia por su parte como se verá después.

b) En segundo lugar, el art. 82 RGPD, contiene en su apartado tercero una cláusula de exoneración de responsabilidad en cuya virtud "El responsable (o encargado del tratamiento) estará exento de responsabilidad *si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios*". Este párrafo lleva a algunos autores, nuevamente, a interpretar que el art. 82 instaura un régimen de responsabilidad subjetiva con inversión de la carga de la prueba, de modo que, si bien la culpa del infractor se presume, éste puede exonerarse demostrando que empleó toda la diligencia debida para evitar el daño[18].

---

15 El principio de responsabilidad proactiva pretende garantizar que todo tratamiento de datos cumpla con el conjunto de la normativa aplicable. Para ello el responsable del tratamiento debe integrar, en sus prácticas internas y en sus sistemas de información, todas las medidas necesarias para obtener tal resultado y alcanzar la eficiencia en la protección de datos personales. Sobre ello vid. SANTOS MORÓN, "Tratamiento de datos. Sujetos implicados. Responsabilidad proactiva", en *Protección de datos personales*, APDC, Tirant lo Blanch, Valencia, 2020, pp. 48 y ss.

16 En este sentido, LÓPEZ DEL MORAL ECHEVERRÍA, "Derecho al resarcimiento por los perjuicios derivados de infracciones en materia de protección de datos…" cit, p. 3068.

17 Como observa VAN ALSENOY "Liability under EU Data Protection Law.rom Directive 95/46 to the General Data Protection Regulation", *JPIPITEC*, 2016, 271, p. 283, el RGPD parece presuponer que el responsable del tratamiento está en mejor situación para exhibir evidencias de las medidas que ha adoptado para asegurar que el tratamiento es conforme a la ley, de modo que, una vez que la víctima ofrece indicios de que existe un tratamiento ilícito, se desplaza la carga de la prueba hacia el primero.

18 NIETO GARRIDO, "Derecho a indemnización y responsabilidad" en PIÑAR (dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad*, Madrid, Reus, 2016, p. 561; NUÑEZ GARCÍA "Responsabilidad y obligaciones del responsable del tratamiento", en RALLO LOMBARTE, *Tratado de*

Lo cierto es, sin embargo, que el art. 82,3 RGPD en ningún momento dice que el responsable o encargado de tratamiento que haya infringido la normativa aplicable puede exonerarse de responsabilidad demostrando que actuó diligentemente. Lo que prevé es que podrán exonerarse si demuestran que no son "responsables" *del hecho* causante del daño, es decir, que pueden exonerarse si prueban que tal hecho *no les es imputable* (atribuible)[19]. En realidad, el art. 82,3 RGPD viene a establecer lo mismo que el art. 23,2 de la Directiva 95/46, que disponía que "el responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra *que no se le puede imputar el hecho que ha provocado el daño*". Este precepto, según el Cdo. 55 de la Directiva sólo permitía al responsable del tratamiento exonerarse de responsabilidad en caso de fuerza mayor o de acto del interesado, pero no mediante la prueba de su diligencia[20]. De acuerdo con ello debe entenderse que el responsable o encargado del tratamiento podrán exonerarse si prueban que el incumplimiento normativo se debe *a un evento ajeno a su ámbito de control*[21], esto es, si ha sido provocado por el comportamiento de la víctima o por causas de fuerza mayor[22].

Protección de Datos, Valencia, Tirant lo Blanch, 2019, p. 384; BUSTO LAGO, ob. cit, pp. 481 y ss.

19 Esto es lo que se deduce de las versiones, francesa e italiana del art 82.3 RGPD que dicen, respectivamente: "Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que *le fait qui a provoqué le* dommage *ne lui est nullement imputable*" y "Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 *se dimostra che l'evento dannoso non gli è in alcun modo imputabile*".
Parece que los autores de la version Española del RGPD han traducido literalmente el texto inglés del indicado precepto según el cual "A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way *responsible* for the event giving rise to the damage" sin tener en cuenta que el término correcto, en español, no es "responsable" sino "imputable". En la traducción española del art. 23,2 de la Directiva, cuyo texto en inglés es equivalente al de la versión inglesa del art. 82,3 RGPD sí se utilizó, sin embargo, el término "imputar".

20 En la Propuesta de Directiva se admitía la posibilidad de que el responsable pudiera exonerarse probando su diligencia (la adopción de "medidas apropiadas" para cumplir las exigencias de los arts 18 y 22). Sin embargo, a lo largo del proceso legislativo, se suprimió esta posibilidad, limitándose los supuestos de exoneración a los indicados. Vid. VAN ALSENOY, ob cit., p. 276; RUBÍ PUIG, ob. cit., p. 79.

21 Obsérvese que el responsable del tratamiento incurre en responsabilidad frente a la víctima con independencia de que el incumplimiento normativo haya sido cometido por el encargado del tratamiento o por un auxiliar o empleado suyo (del responsable del tratamiento). Como ya se indicó, aun en los casos en que

De lo expuesto se desprende que, en el supuesto en que se lleve a cabo un tratamiento de datos que –al menos aparentemente- no es conforme a la ley, corresponde al responsable del tratamiento demostrar el cumplimiento normativo. Si no lo hace y se concluye que existe una infracción, deberá indemnizar a aquél que haya sufrido un daño, a menos que pueda probar que dicha infracción no le es imputable y se debe a un hecho ajeno a su ámbito de control. Desde este punto de vista, puede entenderse que la responsabilidad derivada del art. 82 RGPD es de carácter objetivo pues, constatada la infracción, el RT incurrirá en responsabilidad

La interrogante que surge a continuación es en qué casos existe un incumplimiento normativo, es decir, cuándo el comportamiento del responsable del tratamiento puede constituir una infracción. Para ello es necesario conocer qué deberes incumben al responsable del tratamiento en aplicación del principio de "responsabilidad proactiva" (art. 24 RGPD), que, como sabemos, le obliga a garantizar que el tratamiento de datos es conforme al RGPD.

A grandes rasgos y, sintéticamente, puede decirse que el responsable del tratamiento debe:

a) *Asegurarse de que el tratamiento respeta los principios enunciados en el art. 5 RGPD*. Esto es, los principios de licitud, lealtad y transparencia (art. 5,1, a); limitación de la finalidad (art. 5,1,b); minimización (art. 5,1,c) exactitud (art. 5,1,d); limitación del plazo de conservación (art. 5,1,e); integridad y confidencialidad (art. 5,1, f)[23].

---

pueda existir responsabilidad del encargado (lo que requiere que ha incumplido obligaciones que le son específicamente exigibles, art. 82,2 RGPD) el responsable del tratamiento responderá, como regla, solidariamente junto con él (art. 82,4 RGPD, art. 30,2 LOPD).

Por otra parte, la responsabilidad se hace pesar sobre la persona física o jurídica q*ue tenga la condición de responsable* del tratamiento infractor (cfr. art. 4,7 RGPD), ya que es quién debe garantizar que el tratamiento es conforme con la normativa de protección de datos (art. 24 RGPD). De ahí que sea indiferente que el concreto comportamiento causante del daño haya sido causado por una persona integrada en su empresa u organización. Desde este punto de vista, puede decirse que el responsable del tratamiento responde por los hechos de sus "auxiliares" o "empleados" objetivamente.

22 Víd. VAN ALSENOY, ob. cit., p. 283.

23 El art. 5,2 indica expresamente que el responsable del tratamiento debe garantizar que el tratamiento cumple los mencionados principios: "el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva)".

b) *Respetar los derechos de los interesados* (acceso, rectificación, cancelación, oposición, portabilidad, arts. 15 a 22 RGPD). Para ello es preciso que el responsable del tratamiento articule los medios necesarios para que los interesados puedan ejercer esos derechos, debiendo, además, informarles al respecto.
c) *Adoptar las medidas apropiadas para garantizar un nivel de seguridad* adecuado al riesgo inherente a ese tipo de tratamiento (art. 32 RGPD)[24].

Pues bien, de un análisis preliminar de las mencionadas obligaciones[25], parece desprenderse que, mientras que algunas de ellas pueden calificarse como obligaciones de "resultado" (así sucede con el deber de garantizar que se respeten algunos de los principios del tratamiento)[26], en otros casos sólo se exige al responsable la adopción de medidas "apropiadas" o razon-

---

24 Este deber conlleva otras obligaciones, de carácter accesorio, como la de llevar a cabo *una evaluación de impacto* cuando, en un análisis inicial del riesgo, se detecta que éste es elevado (art. 35 RGPD) o la obligación de consultar a la autoridad de control cuando el resultado de la evaluación de impacto muestre un riesgo elevado que el responsable considere inviable mitigar (art. 36 RGPD).

25 Conviene advertir que, para determinar con certeza cuándo estamos ante una obligación de medios y cuándo ante una de resultado sería necesario realizar un análisis exhaustivo de las distintas obligaciones del responsable del tratamiento. La naturaleza de este trabajo impide llevar a cabo esta tarea por lo que nos limitaremos a enunciar distintos ejemplos de obligaciones de medios y de resultados a fin de ilustrar la hipótesis que manejamos.

26 Del art. 5,2 RGPD, que dispone que "el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo" se desprende que el responsable del tratamiento queda obligado a obtener un *resultado.* No obstante, ello es así siempre y cuando de la definición del concreto principio del tratamiento no se deduzca lo contrario.
Así sucede, por ej., en relación con el principio de exactitud, ya que el art. 5,d), tras disponer que los datos personales deben ser "exactos y, si fuera necesario, actualizados", añade que "se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan". La doctrina estima, a la vista de ello, que el responsable del tratamiento debe implementar procedimientos para actualizar la información y comprobar su exactitud a fin de proceder, en su caso, a la rectificación o eliminación de los datos tratados [TRONCOSO, "Los principios relativos al tratamiento (Comentario al art. 5 RGPD y al art. 4 LOPDGDD)", en *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de Derechos digitales*, t. I, Cívitas-Thomson, 2021, p. 888-889]. De ahí cabe deducir que la mera inexactitud de los datos personales no genera responsabilidad, sino sólo aquella que tenga su origen en la no adopción de medidas razonables para comprobar la exactitud de los datos y rectificarlos o eliminarlos de no ser exactos.

ables dirigidas a obtener tal resultado[27]. Por otra parte, y esto se aprecia especialmente cuando el responsable del tratamiento debe decidir si ha de darse una respuesta positiva a la solicitud de ejercicio de un derecho por parte del interesado, hay casos en que el responsable del tratamiento debe llevar a cabo una labor de ponderación cuyo resultado (equivocado o no) es el que puede determinar la existencia de una infracción. Veamos algunos ejemplos a continuación:

1) Una empresa comercializa una app que permite gastar bromas telefónicas. El usuario de la app graba un mensaje de teléfono con el contenido de la broma y lo envía al destinatario elegido. La app permite grabar la conversación resultante, con la reacción del destinatario de la broma, de modo que luego el usuario (esto es, quien ha gastado la broma) pueda descargarla y difundirla. La grabación se realiza sin consentimiento del afectado[28]. Este supuesto refleja un caso claro de incumplimiento de la normativa de protección de datos: se lleva a cabo un tratamiento de datos (la voz se considera un dato personal) sin consentimiento del interesado y sin que exista otra base de legitimación. Se estaría, en este caso, infringiendo el principio de licitud (art. 6 RGPD) que obliga a contar con el consentimiento del interesado cuando no existe otra base de legitimación[29]. El deber del responsable del tratamiento de obtener dicho consentimiento y de que éste cumpla las condiciones necesarias para su validez (v. gr. emitido de forma afirmativa y tras la necesaria información –cfr. art. 4,11 RGPD-) debe considerarse una obligación de resultado[30]. Las causas por las que no se

27 VAN ALSENOY, ob.cit., p. 282; RUBÍ PUIG, ob. cit., p. 58.

28 Únicamente, al final de la grabación, cuando se constata que se trata de una broma, se pregunta al receptor si se opone a que se lleve a cabo el almacenamiento de sus datos. Este supuesto está basado en los resueltos en las SSTS (Sala 3ª) 18 junio 2020 (RJ 2020/2075); y 22 junio 2020 (RJ 2020/273 y RJ 2020/3593). Todas ellas, emitidas en un procedimiento administrativo sancionador, consideraron que procedía sancionar a la empresa recurrente.

29 Estas bases de legitimación son las siguientes: el tratamiento es necesario para la ejecución de un contrato; es necesario para el cumplimiento de una obligación legal; es necesario para proteger intereses vitales del interesado u otra persona física; es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, o, por último, es necesario para la satisfacción de intereses legítimos del responsable del tratamiento o de un tercero.

30 La única excepción la encontramos en relación con el consentimiento de los menores de edad. Cuando el menor tiene una edad inferior a la prevista legalmente (14 años en España) el consentimiento debe ser emitido por los titulares de la patria potestad o tutela (art. 8,1 RGPD). Pero, dadas las dificultades para comprobar la veracidad de la edad del menor y, por consiguiente, cuándo el

haya recabado el consentimiento –por ej. se estimaba, erróneamente, que no se trataban datos personales, pese a haber recibido asesoramiento legal- son irrelevantes ya que, si no existe base de legitimación, el tratamiento de datos es ilícito. Tal infracción dará lugar a responsabilidad, siempre y cuando exista daño indemnizable (cuestión a la que nos referiremos después).

2) Lo mismo sucede en otros casos de infracción de los principios del tratamiento, como puede ser el principio de minimización. Supongamos que una entidad concede ciertas ayudas a personas que tienen a su cargo a una persona con discapacidad y, de acuerdo con las normas de la convocatoria, publica en internet el listado de los beneficiarios. Pero difunde también los datos de las personas con discapacidad a su cargo. En este caso estaría infringiendo el principio de minimización[31], que implica que el responsable del tratamiento debe recoger y tratar solo los datos indispensables para lograr la finalidad perseguida con el tratamiento[32]. Nuevamente, este comportamiento, por sí mismo, es decir, sin necesidad de enjuiciar la culpa o negligencia del responsable del tratamiento, determina una infracción susceptible de generar responsabilidad.

3) La situación resulta diferente, en cambio, si pensamos en el deber del responsable del tratamiento de implementar las medidas técnicas y organizativas "apropiadas" para garantizar la seguridad del tratamiento (art. 32 RGPD). Puede ocurrir que, aunque el responsable del tratamiento haya

---

consentimiento debe ser prestado por sus padres o tutor, el art. 8,2 RGPD dispone que "el responsable del tratamiento *hará esfuerzos razonables* para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible".

31 El ejemplo está basado en el supuesto resuelto por la STS (Sala 3ª) de 9 de marzo de 2015 (RJ 2015/1298), que sancionó a la Xunta de Galicia (en este caso se trataba de una entidad pública) por publicar un listado de esas características accesible de manera generalizada en internet. Estima la sentencia que, aunque la norma que regulaba las subvenciones (Ley 38/2003) obligaba a publicar los beneficiarios de las mismas, esto no permitía, sin embargo, publicar también los datos de las personas con discapacidad tomadas en consideración para otorgar la subvención. En este caso, además, se entiende que los datos sobre la discapacidad, en tanto datos relativos a la salud, debían considerarse datos "especialmente protegidos" de acuerdo con la normativa entonces vigente (en la actualidad quedarían englobados entre las "categorías especiales de datos personales" a que alude el art. 9 RGPD).

32 Según el art. 5,1,d los datos deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

hecho cuanto está en su mano para ofrecer un entorno seguro, y, por consiguiente, haya adoptados medidas "apropiadas[33], éste sea hackeado por un tercero. Esto es lo que ocurrió en el supuesto resuelto por la SAN de 25 de febrero de 2010 (JUR 2010/82723). Un sujeto con altos conocimientos técnicos rompió los sistemas de seguridad establecidos por los responsables de un portal (www.portallatino.com), descargando los datos de usuarios de dicho sitio web que difundió luego en internet. La sentencia, emitida en el seno de un procedimiento administrativo sancionador, considera que los responsables del portal habían adoptado medidas de seguridad adecuadas por lo que no podía responsabilizárseles del acceso indebido del tercero a los ficheros[34].

Teniendo esto en cuenta, para considerar infringido el deber de adoptar las medidas de seguridad "apropiadas" al tratamiento es necesario valorar la culpa o negligencia del responsable del tratamiento. Es decir, estaríamos en este caso ante una obligación de medios, y así lo afirma la STS (Sala 3ª) de 15 de febrero de 2022 (RJ 2022/1280), que niega que, producida una filtración de datos personales, pueda existir responsabilidad (en este caso de carácter sancionador) con independencia de las medidas adoptadas y la actividad desplegada por el responsable del tratamiento (FJ 3º).

4) Otro de los deberes que incumbe al responsable del tratamiento es el de respetar los derechos de los interesados. En relación con ellos, cabe distinguir diversas situaciones. Hay determinadas obligaciones que pueden considerarse incumplidas por el mero hecho de no obtener el resultado exigido en la norma. Si el responsable del tratamiento, contrariando lo

33 Según el art. 32 RGPD el responsable (y el encargado) del tratamiento deben adoptar las medidas en cuestión teniendo en cuenta el *riesgo* que, para los derechos de las personas físicas, genera ese concreto tratamiento (en función de su naturaleza, alcance, contexto y fines) , así como el estado de la técnica y los costes de aplicación.

34 Según dicha resolución, la intrusión en los sistemas de Portal Latino "no responde a una falta o ineficacia de las medidas de seguridad sino a una actitud activa e intrusiva por parte de un hacker". De ahí que concluyera que no podía imputarse a la mencionada entidad la infracción, recogida en la anterior LOPD (art. 44, 3, h) consistente en no mantener "las debidas condiciones de seguridad".
En cualquier caso, pese a considerar que las medidas de seguridad adoptadas por la entidad denunciada eran apropiadas, estimó que su comportamiento posterior, una vez tuvo conocimiento del acceso del hacker a su sistema, había sido negligente, ya que "no realizó actividad alguna, pese a que era consciente del riesgo de una posible revelación o publicidad del fichero" por lo que finalmente su comportamiento fue objeto de sanción.

establecido en el art. 12,2 LOPD[35], no informa a los interesados sobre los medios a su disposición para ejercitar los derechos que se le reconocen, estaremos ante un incumplimiento normativo. Si realizada una solicitud por un interesado, el responsable del tratamiento no emite respuesta alguna, se estará incumpliendo lo establecido en el art. 12,4 LOPD[36], que le impone el deber de responder. Ahora bien, la decisión en torno a si el derecho ejercitado por el interesado debe ser o no satisfecho requiere en ocasiones cierta labor de ponderación[37]. Y ello implica que la existencia o no de infracción va a depender de que la valoración realizada por el responsable del tratamiento se considere o no acertada. Esto se aprecia, particularmente, en relación con el derecho de supresión, que, como se sabe, engloba el denominado "derecho al olvido". Uno de los supuestos en que el interesado tiene derecho a que se supriman sus datos personales es aquél en que los mismos *ya no son necesarios en relación con los fines para los que fueron recogidos o tratados* (art. 17.1,a). Este supuesto es, justamente, el que, a tenor de la jurisprudencia europea (STJU 13 mayo 2014, caso Google-Spain) fundamenta el derecho al olvido. Como se sabe, este derecho permite exigir que se eliminen de la lista de resultados de los buscadores datos del interesado, cuando dicha información, aun siendo inicialmente lícita, pueda considerarse, en el momento de ejercicio del derecho, *inadecuada o excesiva en relación con los fines del tratamiento*. Para determinar que así es debe tenerse en cuenta la relevancia pública o no de la persona afectada y el tiempo transcurrido, ya que estas circunstancias son los que pueden determinar que la subsistencia de la información resulte injustificada, por no existir ya interés público en el acceso a la misma.

---

35 Según este precepto "El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio".

36 Art. 12.4: "La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable".

37 Tal labor de ponderación no parece que entre en juego cuando se trata del derecho de acceso, cuyo ejercicio obliga al responsable a confirmar si está tratando datos personales del interesado y facilitarle una copia de éstos (art. 15 RGPD, 12 LOPD). Tampoco en el supuesto del derecho de rectificación (art. 16 RGPD, 14 LOPD) que obliga al responsable del tratamiento a rectificar, sin dilación, los datos inexactos o completar los incompletos, ni cuando se trata del derecho a la portabilidad. Puede ser necesaria, en cambio, cuando se ejercita el derecho de supresión y el derecho de oposición.

Pues bien, uno de los pocos supuestos en que se han ejercitado, en el Derecho español, acciones de responsabilidad por incumplimientos de la normativa de protección de datos, es el referido al ejercicio sin éxito del derecho al olvido[38]. Y el que la acción de responsabilidad haya o no prosperado depende de que el tribunal enjuiciador considere que la decisión de la entidad demandada, negándose a satisfacer la solicitud del interesado, es o no acertada. Así, mientras que en las Sentencias de la Sala civil del TS, 545/2015 de 15 de octubre (RJ 2015/4417)[39] y 210/2016 de 5

38 En estos casos el demandante suele ejercitar una acción por intromisión en sus derechos al honor y a la intimidad, además de por vulneración al derecho a la protección de datos, ya que se sostiene que el hecho de no eliminar la información a la que se refiere el derecho al olvido, trae consigo la vulneración de sus derechos a la intimidad y honor.

39 Esta sentencia (del Pleno) es la primera que aborda, en el ámbito civil, el ejercicio del "derecho al olvido". La demanda se ejercitó en este caso frente al editor de un periódico digital (no frente a un motor de búsqueda) que había publicado en su hemeroteca digital una noticia, fechada muchos años atrás, sobre la condena por tráfico de drogas de dos personas totalmente rehabilitadas en el momento de ejercicio del derecho al olvido. Los afectados solicitaron al editor que adoptara medidas para evitar la indexación de la noticia por motores de búsqueda, que adoptara también medidas para evitar que la información fuese indexada dentro del propio motor de búsqueda de la hemeroteca y, asimismo, que eliminara sus nombres y apellidos de la noticia original. El TS consideró que, si bien la eliminación del nombre y apellidos de las personas afectadas en la noticia original era un sacrificio desproporcionado de la libertad de información, la negativa del editor del periódico demandado a adoptar medidas para evitar la desindexación por motores de búsqueda supuso una vulneración de su derecho a la protección de datos y una intromisión en sus derechos a la intimidad y al honor, condenando, por tanto, a la entidad demandada a abonar la correspondiente indemnización. Y ello porque estimó, que, en ese caso, el tiempo transcurrido, unido a la falta de relevancia pública de las personas referidas en la noticia en cuestión, privaban a dicha información de interés público. Concluyó en suma que "el tratamiento de datos" que llevaba a cabo el editor del periódico en su hemeroteca digital no era adecuado a la finalidad del tratamiento inicial. Esta sentencia, al no atender a la petición de los demandantes de que se eliminaran sus nombres de la noticia original y se prohibiera indexarla en el motor interno de la hemeroteca digital fue recurrida por éstos ante el TC. El TC, en su S. 58/2018 de 4 de junio, reiteró la postura del TS en cuanto a la posibilidad de que una noticia, que inicialmente tiene interés general (en cuyo caso prevalece el derecho a la libertad de información frente a los derechos fundamentales del afectado), pueda devenir carente de interés público por transcurso del tiempo. Pero, a diferencia del TS, consideró que la prohibición de indexar datos personales en el motor de búsqueda interno del periódico era una medida proporcionada (no así la relativa a la supresión del nombre y apellidos de los actores en la noticia en cuestión).

abril (RJ 2016/1006)[40], se condenó a la entidad demandada a indemnizar al afectado, por entenderse que debía haber atendido su petición, en otros casos se ha llegado a la conclusión contraria. Así, por ej. las Sentencias (Sala civil) 426/2017 de 6 de julio (RJ 2017/3194) y 446/2017 de 13 de julio (RJ 2017/3623) desestimaron la acción de responsabilidad ejercitada contra el demandado frente a diversos medios de prensa que habían publicado una noticia que le afectaba, por entender que su solicitud de eliminación de información y prohibición de indexación no encajaba en los supuestos de "derecho al olvido" y además la noticia no había perdido interés público[41]. El Auto del TS de 4 de abril de 2018 (JUR 2017/94850) inadmitió

40 En ese caso el demandante había solicitado a Google (además de a otros buscadores) que adoptara medidas para evitar la indexación de información sobre un indulto del que fue beneficiario en 1999 (el delito por el que fue indultado se cometió en 1981). La petición fue realizada en 2009, pero Google se negó a atenderla, por lo que el demandante presentó una reclamación ante la AEPD. A pesar de que la AEPD estimó la reclamación contra Google, el buscador no eliminó los datos de su lista de resultados. Por tal motivo el demandante, en 2011, demandó a dicha compañía, que fue condenada por la Audiencia Provincial por entender que se había producido un incumplimiento de la normativa de protección de datos. Recurrida la sentencia por el demandado, el TS confirmó la sentencia de la AP, aclarando que Google no vulneró la normativa de protección de datos cuando inicialmente enlazó a la página web con información sobre el indulto sino, cuando, 10 años después de su publicación, y tras ser requerida para cancelar tal tratamiento de datos, no llevó a cabo tal cancelación. Señala la sentencia que un tratamiento inicialmente lícito puede dejar de serlo con el plazo del tiempo. Y esto es lo que sucedió en el caso enjuiciado, en el que se entendió que el tratamiento de datos consistente en el enlace a la noticia del indulto devino inadecuado para la finalidad inicial.

41 En diversos medios de prensa (que fueron demandados) se publicó una noticia acerca del juicio seguido contra el presunto autor de dos asesinatos, en la que se informaba de la inexistencia de suficientes pruebas para condenarlo. En el artículo periodístico no se mencionaba el nombre ni los apellidos del enjuiciado, solamente aparecía su imagen tomada en la Sala de vistas. El afectado ejercitó una acción indemnizatoria contra los editores de los periódicos en cuestión por intromisión a su derecho al honor (y, erróneamente, "imagen") invocando además su derecho al olvido a fin de solicitar que se retirara su imagen de todos los archivos informáticos que la pudieran alojar, así como buscadores y redes sociales. Respecto de este último el TS señala que el derecho al olvido no ampara la eliminación de información en la noticia original (esto ya lo había afirmado en la mencionada S. de 15-10-2015) y, dado que el único dato personal objeto de tratamiento era la imagen del demandante, no cabía la búsqueda por su nombre y apellidos por lo que no procedía tampoco su petición de no indexación. Entendió además que no concurría en ese caso el requisito de desaparición del interés público de la información. Consideró que los hechos acaecidos eran de extraordinaria

el recurso contra la sentencia de la AP que desestimó la acción indemnizatoria ejercitada por el demandante contra Google. El demandante había solicitado que Google retirase de su lista de resultados información relativa a un delito contra la Hacienda pública por el cual fue condenado y posteriormente indultado, ejercitando además contra dicha entidad una acción indemnizatoria por vulneración de su derecho a la protección de datos personales, a la intimidad y al honor. La sentencia de la AP consideró que el demandante, que figuraba en la lista Falciani, tenía la consideración de "personaje público" por lo que, atendiendo a la jurisprudencia del TS, no estaba amparado por el derecho al olvido, ni existía intromisión en los derechos invocados.

Lo expuesto permite poner de manifiesto que el debate en torno a la naturaleza, objetiva o por culpa, de la responsabilidad por incumplimiento de la normativa de protección de datos, no es del todo acertado. La cuestión relevante es determinar cuándo existe un incumplimiento normativo. Y, mientras que en ciertos la mera omisión de una conducta (v. gr. no responder una solicitud de ejercicio de un derecho; no informar al interesado de que se están tratando sus datos personales) o la no obtención de determinado resultado (v. gr. existencia de una base de legitimación para el tratamiento de datos) determinan la existencia de una infracción normativa, en otros casos, puede ser necesario valorar el grado de diligencia del responsable del tratamiento (a la hora, por ej. de adoptar medidas de seguridad) o evaluar el juicio de ponderación realizado por éste (v. gr. al decidir si satisface o no el derecho ejercitado por el interesado).

3. Acerca de la existencia de daño

Un requisito indispensable para que exista deber de indemnizar es la existencia de daño, que, conforme al art. 86 RGPD puede ser material o inmaterial. Sin embargo, ha de tenerse en cuenta que no todo incumplimiento de la normativa de protección de datos genera automáticamente un perjuicio[42].

En los casos en que el incumplimiento de la normativa de protección de datos provoca una intromisión en el derecho a la intimidad o al honor

gravedad e impacto social y la noticia seguía teniendo actualidad, dado que sólo habían transcurrido dos años desde la que tuvo lugar el procedimiento judicial.

42 Así lo afirma la SAP Barcelona 364/2014 de 17 de julio (AC 2014/1661) que fue luego confirmada por el TS en su Sentencia, ya mencionada, de 5 de abril de 2016.

del afectado, no hay duda de que se produce un daño que será, en todo caso, de carácter moral, ya que la ley española presume la existencia de dicho daño siempre que se lesiona el derecho al honor, a la intimidad o a la imagen (art. 9,3 LO 1/92). No hay que descartar que en ese supuesto se produzcan además, daños económicos (v. gr. derivados de la pérdida de la reputación profesional) pero tales daños deberán ser objeto de prueba.

Ejemplos de infracciones de la normativa de protección de datos que traen consigo la lesión de otros derechos de la personalidad son los consistentes en la inclusión indebida de una persona en un fichero de morosos[43], o la no satisfacción del derecho al olvido cuando debía haber sido atendido este derecho[44]. La vulneración del deber de confidencialidad[45] con el consiguiente acceso de terceros no autorizados a los datos del interesado,

---

43 Los requisitos para que sea lícita la inclusión de un sujeto en un fichero negativo de solvencia vienen establecidos en España en la LOPD (antes en la Ley 1998 y ahora en la LOPD 2018) de manera que, si no se cumplen esos requisitos, se considera vulnerado el derecho al honor. Son muchas las sentencias que han condenado a indemnizar a la persona cuyos datos fueron publicados en un fichero de morosos, cuando la deuda era controvertida o incierta. Los tribunales han venido entendiendo que en esos casos no se cumplía con el "principio de calidad" (que con anterioridad al RGPD se consideraba referido a la necesidad de "adecuación, pertinencia, proporcionalidad y exactitud" de los datos objeto de tratamiento) y, por tanto, el tratamiento de datos personales que conlleva la inclusión en un fichero de solvencia no era lícito y traía consigo una lesión del derecho al honor del afectado. Vid. DÍEZ SOTO, "El régimen de los sistemas de información crediticia en la nueva legislación sobre protección de datos", en *Protección de datos personales,* APDC, Valencia: Tirant lo Blanch, 2020, pp. 505 y ss.

44 En España el derecho al olvido se ha ejercitado tanto frente a motores de búsqueda como frente a editores de medios de prensa. No obstante, conviene advertir que en este segundo caso el ejercicio del derecho al olvido permite obtener del medio de prensa la adopción de medidas para evitar la indexación, por parte de los motores de búsqueda, de la información que atañe al interesado, pero no obtener la eliminación de los datos personales del interesado en la noticia publicada por el medio de prensa de que se trate.

45 La vulneración de la confidencialidad de los datos puede deberse al acceso indebido a los datos por parte de un tercero –lo que, a su vez, puede tener su origen en la falta de adopción de las necesarias medidas de seguridad o en la actuación de un tercero ajeno al ámbito de control del responsable- pero también a la cesión o comunicación voluntaria de los datos, por parte del responsable del tratamiento, a un tercero. La anterior LOPD prohibía la cesión de datos realizada sin consentimiento del afectado salvo en los supuestos previstos en el art. 11.2. Ni el RGPD ni la actual LOPD aluden a la cesión o comunicación ilícita de datos personales pero es claro que este comportamiento supone un vulneración del deber de confidencialidad al tiempo que implica un tratamiento de datos ilícito por carecer de base de legitimación.

puede suponer, igualmente una lesión en su derecho a la intimidad y/o al honor (aunque ello dependerá de los datos concretos que hayan sido objeto de tratamiento indebido). Pensemos en el supuesto en que un fichero con datos personales de enfermos de un hospital resulta accesible desde una página de internet[46], lo que afecta claramente a su intimidad, o en el supuesto en que una empresa comunica a otra, que mantiene un base de datos de "trabajadores conflictivos", que ha despedido a uno de sus trabajadores debido a su "mal comportamiento" (es evidente que la inclusión del mencionado trabajador en un fichero de tales características afecta negativamente su reputación).

En tales situaciones, además de daño moral, puede existir, como antes se indicó, daño patrimonial. Es el caso del supuesto que se acaba de enunciar, resuelto por la Sentencia de la Sala civil del TS 6091/2015 de 12 noviembre 2015 (RJ 2015/5603)[47], que condenó al demandado a indemnizar al actor por daño moral y por daño patrimonial. En este caso el daño patrimonial resultaba de las dificultades que padeció el afectado para ser contratado por empresas del sector, si bien, pese a la necesidad de que el daño sea cuantificado, el TS lo calculó de manera "estimativa" otorgando una indemnización –por daño moral y patrimonial- de 30.000 euros[48].

---

46 Este supuesto se inspira en el resuelto por la STS (Sala 3º) 20 noviembre 2012, RJ 2013/309, en un procedimiento administrativo sancionador. En esta hipótesis se consideró infringido, de un lado, el deber de adoptar las medidas necesarias para garantizar la seguridad del tratamiento (art. 9 de la anterior LOPD de 1999) y, de otro, el "deber de secreto" consagrado en el art. 10 de la LOPD 1999, equivalente al actual deber de confidencialidad, aunque en realidad la sanción (que no podía ser doble) se impuso por la comisión de la segunda infracción.

47 Un sujeto fue despedido por su empresa, dedicada a la instalación de tendidos telefónicos, por una causa injustificada (el despido fue declarado improcedente). Pese a ello, la empresa en cuestión, que solía trabajar para Telefónica, comunicó a esta que había despedido a su empleado debido a su carácter conflictivo. El hecho de que Telefónica incluyera a dicho sujeto en su fichero de "trabajadores conflictivos" imposibilitaba su contratación por cualquier empresa que trabajara para telefónica. El afectado demandó a la empresa informante por vulneración de la normativa de protección de datos y lesión de su derecho al honor, solicitando una indemnización por daño moral y económico. El TS consideró que se había vulnerado el derecho fundamental del demandante a la protección de sus datos de carácter personal porque la cesión de datos fue ilícita, los datos cedidos no eran, además, veraces, y no se concedió al demandante la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

48 El demandante solicitó una indemnización de 653.310,56 euros, resultante de multiplicar su sueldo base por los meses (374) que mediaban entre que fue despedido y finalizó su vida laboral. Esta indemnización fue considerada desproporcionada por el TS, que observó que la dificultad del actor para encontrar

Pero ¿qué sucede cuando nos enfrentamos ante un tratamiento de datos que incumple algún aspecto de la normativa aplicable pero del cual no se deriva una lesión el derecho al honor, la intimidad o la imagen? Supongamos que una red social recaba el consentimiento de sus usuarios para tratar sus datos personales, pero no le informa de todos los extremos que establece la ley (concretas finalidades del tratamiento; derechos que le corresponden, etc. cfr. art. 13 RGPD y art. 11.1 LOPD), es decir, se infringe el principio de transparencia. ¿Podría ejercitar el usuario una acción de responsabilidad frente al proveedor de la red social?. En mi opinión en estos casos, existe, cuando menos, un daño moral derivado de la vulneración del derecho a la protección de datos personales.

Debe tenerse en cuenta que el derecho a la protección de datos personales, aunque suele relacionarse con la protección de la intimidad, tiene la consideración de derecho fundamental autónomo[49]. Tal y como ha sido definido por el TC (S. 290/2000 de 30 de noviembre) es un derecho que atribuye a las personas físicas "el *poder de disposición sobre sus propios datos*, *sean o no íntimos*, siempre que vayan a estar sometidos a tratamiento, informatizado o no". De ahí que pueda ser configurado como un derecho de la persona a "controlar" los datos que le atañen -que se sustancia en la facultad de consentir la recogida, la obtención y el acceso a esos datos, su posterior almacenamiento y tratamiento, así como su uso o usos posibles-[50]. Por

---

trabajo en empresas del mismo sector en que había venido trabajando, dada su edad y cualificación, no suponía su total exclusión del mercado laboral. Por ello el TS optó por fijar (de manera un tanto cuestionable) "estimativamente" una indemnización dirigida a cubrir el daño moral y el patrimonial.

49 En España el derecho a la protección de datos personales (en su momento denominado por algunos autores derecho a la "autodeterminacación informativa", cfr. MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990) tiene su anclaje en el art. 18,4 CE, que dispone que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". No obstante, la configuración actual del derecho a la protección de datos personales va más allá pues se concibe, como se indica en el texto, como un derecho autónomo y no un mero instrumento para la protección de otros derechos fundamentales.

50 PIÑAR, "Comentario al art. 3 LOPD", en *Comentario a la LO de Protección de datos de carácter personal*, Cívitas-Thomson, 2010, p. 57. DEL CASTILLO VÁZQUEZ "Requisitos del consentimiento utilizado como fundamento jurídico para el tratamiento de los datos de carácter personal (Comentario al art. 7 RGPD y al art. 6 LOPDGDD), en TRONCOSO (dir.) *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos peronales y Garantía de los Derechos digitales*, t. I, Cicur-Menor, Cívitas-Thomson, 2021, p. 947, señala, en este sentido, que el contenido esencial de este derecho otorga a su

ello, toda infracción que conlleve la pérdida o disminución del poder del individuo de controlar sus datos personales lesiona el núcleo esencial del derecho a la protección de datos personales. Esto es lo que, ocurre, en mi opinión, cuando se vulneran los principios del tratamiento y los derechos reconocidos al interesado, por lo que, en tales hipótesis, aunque no se produzca a su vez, una intromisión en la intimidad del afectado (o en otros derechos como su honor o imagen), creo que debe considerarse producido un daño moral[51] que podrá ir o no acompañado, según los casos, de un daño patrimonial.

Ahora bien, esto no significa que todo incumplimiento de la normativa de protección de datos suponga una vulneración del derecho fundamental a la protección de datos personales. Algunos de los deberes impuestos al responsable del tratamiento, en el RGPD o en la LOPD, tienen carácter preventivo o instrumental y están dirigidos a garantizar que se cumple el conjunto de la normativa, mientras que otros se imponen al responsable del tratamiento frente a la autoridad de control.

Ejemplos de ellos son entre otros, el deber del responsable del tratamiento de formalizar un contrato de encargo de tratamiento con el sujeto que vaya a tratar datos por su cuenta (art. 28,3 RGPD); el deber de los corresponsables del tratamiento de formalizar un contrato que regule sus relaciones (art. 26,1 y 2 RGPD); el deber del responsable del tratamiento de disponer de un registro de actividades (art. 30 RGPD), o designar, en los casos establecidos en la ley, un delegado de protección de datos (arts. 37 RGPD y 34 LOPD), o el deber de consultar a la Autoridad de control en caso de tratamiento de alto riesgo (art. 36 RGPD).

El incumplimiento de estos deberes puede no ocasionar ningún daño a la persona o personas cuyos datos son objeto de tratamiento. Si como consecuencia de su incumplimiento no se produce la vulneración de alguno de los principios del tratamiento, la lesión de los derechos del interesado y tampoco se viola la seguridad de los datos, no podrá considerarse vulnera-

---

titular "una posición jurídica de contenido positivo que se conforma sobre un haz de facultades destinadas a controlar el uso de su información personal, tanto en el momento inicial de la recogida de datos, como en fases posteriores del tratamiento" y se materializa en "la libre decisión sobre qué datos propios desea su titular poner a disposición de terceros y qué utilización de los mimos autoriza".

51 Ciertamente no hay ninguna norma, equivalente al art. 9,3 LO 1/82 que presuma dicho daño moral, pero su carácter de derecho fundamental, unido a la amplitud y flexibilidad con que la jurisprudencia valora la existencia de daño moral, debería llevar a admitirlo. Cuestión distinta es su cuantificación, que, como se sabe, queda a discreción del juez.

do su derecho a la protección de datos y será difícil apreciar la existencia de un perjuicio que pueda fundar una acción de responsabilidad[52]. Lo mismo cabe decir del deber de adoptar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (art. 32,1 RGPD) al que se aludió con anterioridad. Este deber pretende garantizar la integridad y confidencialidad de los datos, pero puede ocurrir que, pese a resultar inadecuadas las medidas de seguridad adoptadas, abstractamente consideradas, no se produzca ninguna brecha de seguridad, no se pierdan o eliminen indebidamente datos, ni se produzca un acceso indebido a esos datos por parte de un tercero. De darse esta situación, el incumplimiento de dicho deber, pese a constituir una infracción administrativa susceptible de sanción[53], no generará ningún perjuicio ni, por consiguiente, tendría sentido el ejercicio de una acción de responsabilidad por parte del sujeto cuyos datos son objeto de tratamiento.

52 Todos estos comportamientos están catalogados en la LOPD como infracciones administrativas susceptibles de ser sancionadas.

53 Cabría la posibilidad de que, en una eventual inspección de la AEPD, se estimara que las medidas empleadas por el responsable del tratamiento no son satisfactorias. Este hecho puede dar lugar a una sanción, ya que tal comportamiento está tipificado como infracción administrativa (art. 73,f LOPD). La doctrina administrativa considera que se está ante una infracción "de actividad" o "peligro abstracto", derivada de la mera omisión de medidas adecuadas, de modo que podrá existir infracción aunque llegue a producirse un resultado lesivo. GONZÁLEZ ESPADAS, "Infracciones consideradas graves (Comentario al art. 73 LOPDGDD), ob. cit. pp. 3169 y ss.