Institut de Dret privat europeu i comparat
Universitat de Girona (Coord.)

El Dret civil català davant la transformació digital i les exigències de la sostenibilitat

El Dret civil català davant la transformació digital i les exigències de la sostenibilitat

El Dret civil català davant la transformació digital i les exigències de la sostenibilitat

Institut de Dret privat europeu i comparat Universitat de Girona (Coord.)

Documenta Universitaria

Dades CIP recomanades per la Biblioteca de la UdG

CIP 347(467.1) JOR

Jornades de Dret Català (23es : 2025 : Tossa de Mar, Catalunya)
El Dret civil català davant la transformació digital i les exigències de la sostenibilitat / $$c Institut de Dret privat europeu i comparat Universitat de Girona (Coord.). – Girona : Institut de Dret Privat Europeu i Comparat de la Universitat de Girona : Documenta Universitaria, juny de 2025. – 1 recurs en línia (686 pàgines). Ponències de les XXIIIenes Jornades de Dret Català, celebrades a Tossa de Mar els dies 25 i 26 de setembre de 2025.
– Descripció del recurs: 10 juliol 2025
ISBN 978-84-9984-703-0 (Documenta Universitaria). – ISBN 978-84-8458-539-8 (Oficina Edicions UdG)

I. Universitat de Girona. Institut de Dret Privat Europeu i Comparat
1. Contractes electrònics – Congressos 2. Comerç electrònic – Dret i legislació – Congressos 3. Xarxes socials en línia – Dret i legislació – Congressos 4. Capacitat jurídica – Congressos 5. Consentiment (Dret) – Congressos 6. Protecció de dades – Congressos 7. Reparacions – Dret i legislació – Congressos 8. Desenvolupament sostenible – Congressos 9. Seguretat informàtica – Congressos 10. Criptomoneda – Dret i legislació – Congressos 11. Dret català – Congressos

CIP 347(467.1) JOR

Disseny de la coberta: Documenta Universitaria
Il·lustració de la coberta: Institut de Dret Privat Europeu i Comparat de la Universitat de Girona

www.documentauniversitaria.com
info@documentauniversitaria.com
Documenta Universitaria® d'Edicions a Petició, SL

ISBN Documenta Universitaria
978-84-9984-703-0

ISBN Oficina Edicions UdG
978-84-8458-539-8

DOI: 10.33115/b/9788499847030

Girona, juliol de 2025

Documenta Universitaria
@DocUniv
documentauniversitaria.com

Les Vint-i-tresenes Jornades han estat organitzades per l'Institut de Dret privat europeu i comparat de la Universitat de Girona, en col·laboració amb l'Ajuntament de Tossa de Mar i el suport de:

- Generalitat de Catalunya. Departament de Justícia i Qualitat Democràtica
- Universitat de Girona
- Acadèmia de Jurisprudència i Legislació de Catalunya
- Deganat autonòmic dels Registradors de la Propietat i Mercantils de Catalunya
- Col·legi Notarial de Catalunya
- Facultat de Dret UB (Deganat)
- Facultat de Dret UdG (Deganat)
- Facultat de Dret UPF (Deganat)
- Col·legi de l'Advocacia de Girona
- Col·legi d'Advocats de Terrassa
- Col·legi de l'Advocacia de Figueres
- Col·legi d'Advocats i Advocades de Tortosa

Índex

PONÈNCIES

Ponència inaugural

Primera ponència
Contractació privada i entorn digital

Segona ponència
Contractació privada i sostenibilitat

Tercera ponència
Noves formes de propietat en l'entorn digital

Quarta ponència
La transformació digital de la pràctica jurídica a Catalunya

COMUNICACIONS

DOI: https://doi.org/10.33115/b/9788499847030_14

Reflexiones sobre la responsabilidad civil por brechas de seguridad de datos personales: el caso del Hospital Clínic

Felipe Oyarzún Vargas

Universidad Carlos III de Madrid

Sumario

1. Introducción*

En marzo de 2023, el Hospital Clínic de Barcelona (HCB) sufrió un ciberataque que tuvo una serie de repercusiones. Por un lado, se cancelaron 150 intervenciones y más de 2.000 visitas externas, se llevaron a cabo actividades de forma manual que usualmente se hacen con sistemas tecnológicos y tuvieron que derivar el transporte sanitario urgente hacia otros hospitales.[1] Además, a consecuencia de este ciberataque (tipo *ransomware*[2]), el HCB sufrió el robo masivo de información (4,5 terabytes), afectando la privacidad de pacientes y profesionales del centro sanitario. Los hackers exigieron un rescate de 4,5 millones de euros, que el hospital se negó a pagar, lo que derivó en varias filtraciones de datos personales en los meses de marzo, abril y julio del 2023.[3]

Este asunto ha tomado relevancia nuevamente dado que, en julio de 2024, la Autoridad Catalana de Protección de Datos (APDCAT) ha impuesto una sanción al HCB —en su calidad de responsable del tratamiento[4]— tras concluir que la institución había infringido la normativa de protección de datos, puesto que no disponía de

* Este trabajo ha sido realizado en el marco del Proyecto de Investigación 2024/00700/001 (Proyectos Áreas Temáticas PPIT2024), «El impacto de la inteligencia artificial en el régimen de la responsabilidad civil médica» («IARMED»), financiado por la UC3M (programa propio).

1 Informe de la Generalitat de Cataluña titulado «*La ciberseguretat a Catalunya*», p. 9. En: https://ciberseguretat.gencat.cat/web/.content/06_dadesCiberseguretat/elements-documents/Documents/Ciberseguretat-a-Catalunya-2024_Informe-tecnologic-CAT.pdf

2 Se define como un *software* diseñado por delincuentes para impedir que los usuarios accedan a su propio sistema informático o a sus archivos a menos que paguen dinero. Véase: https://dictionary.cambridge.org/dictionary/english/ransomware

3 En prensa: https://elpais.com/espana/catalunya/2023-07-04/los-ciberdelincuentes-que-atacaron-el-hospital-clinic-filtran-una-tercera-entrega-de-datos.html

4 Aplicando el art. 4.7 del RGPD, se debe indicar que el HCB era el «responsable del tratamiento» dado que era la persona jurídica que determinaba los fines y medios del tratamiento de los datos personales de los pacientes y trabajadores de ese centro sanitario.

las medidas de seguridad necesarias para evitar un ciberataque ni proteger los datos personales de sus pacientes.[5]

Esta situación dista de ser un precedente aislado. España ha sido uno de los países más afectados por ataques de *ransomware* en 2024.[6] En Cataluña es de público conocimiento que cada vez son más las empresas catalanas que han sido víctimas de ciberataques.[7] Según el Instituto Nacional de Ciberseguridad (INCIBE), los ciberataques recibidos en España alcanzaron en 2023 una cifra récord de 83.517 incidentes de ciberseguridad, lo cual representa un incremento de un 24 % respecto al año anterior.[8]

Respecto a la situación en hospitales o centros sanitarios, estos tienen especial trascendencia dado que manejan y almacenan una ingente cantidad de datos personales de pacientes y trabajadores. De hecho, el sector sanitario es uno de los objetivos preferidos por las bandas de *ransomware*, siendo el segundo sector más atacado por tercer año consecutivo tras el sector industrial.[9]

A partir de los antecedentes presentados, se observa que estas situaciones son cada vez más comunes, siendo necesaria una reflexión al respecto. En este trabajo, concretamente, se centrará la reflexión en aspectos de la responsabilidad civil a causa de estos casos en Cataluña.

---

[5] Resolución sancionadora dictada por la APDCAT, n.º PS 1/2024, de 16 de julio de 2024.

[6] Véase: https://cincodias.elpais.com/smartlife/lifestyle/2024-09-17/espana-quinto-pais-mas-ciberataques-recibe.html

[7] Véase: https://www.elperiodico.com/es/sociedad/20211111/ola-ciberataques-empresas-catalanas-robarles-datos-12831804

[8] Documento en: https://www.incibe.es/sites/default/files/2024-08/Infograf%C3%ADa_balance_de_ciberseguridad_INCIBE_2023_0.pdf

[9] Informe «*La ciberseguretat a Catalunya*», p. 11. En: https://ciberseguretat.gencat.cat/web/.content/06_dadesCiberseguretat/elements-documents/Documents/Ciberseguretat-a-Catalunya-2024_Informe-tecnologic-CAT.pdf

2. Sobre el orden jurisdiccional competente y la legislación aplicable

Con el objeto de otorgar ciertas pautas en el tratamiento de datos personales en Cataluña, conviene iniciar las reflexiones haciendo referencia al orden jurisdiccional y la legislación aplicable en este tipo de supuestos.

Con base en el art. 82.6 del Reglamento General de Protección de Datos (RGPD), las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro, de acuerdo con el art. 79.2 del RGPD.[10] De esta forma, en el supuesto de que la víctima ejerza una acción ante tribunales españoles, deberá presentar su demanda en una sede distinta, según cual sea la naturaleza del ente que ha sido el responsable del tratamiento de los datos personales. En caso de ser un ente privado, se deberá presentar una acción ante la jurisdicción civil; en cambio, si es un ente público, deberá presentar su acción ante la jurisdicción contencioso-administrativa.[11]

En el caso objeto de estudio, el HCB pertenece a la Red de Hospitales Públicos de Cataluña, es decir, se está en presencia de una persona jurídica de Derecho Público. En consecuencia, el orden jurisdiccional competente será el contencioso-administrativo, dado

[10] Art. 79.2 RGPD: Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

[11] En igual sentido, Santos Morón, María José, «Reflexiones en torno a la jurisprudencia del TJUE sobre la acción indemnizatoria del art. 82 RGPD», *Cuadernos de Derecho Transnacional*, 2024, 16(2), p. 1406; López del Moral Echeverría, José Luis, «Derecho al resarcimiento por los perjuicios derivados de infracciones en materia de protección de datos (Comentario al artículo 82 RGPD)», en Antonio Troncoso Reigada (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*, Vol. 2, Pamplona: Civitas, 2021, p. 3073.

que la lesión de los derechos de los interesados se debe al tratamiento de datos llevado a cabo por un responsable que es un ente público.[12]

Una vez definido el orden jurisdiccional competente, es preciso apuntar algunas cuestiones respecto a la normativa aplicable, teniendo especial consideración en los supuestos donde el responsable del tratamiento es un ente público.

España no ha incluido una norma especial de responsabilidad civil en materia de protección de datos, a diferencia de otros ordenamientos jurídicos.[13] A diferencia de lo que ocurría en la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (la cual establecía una regla de responsabilidad en su art. 19[14]), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD) no contiene ninguna disposición al respecto.

[12] Villalba Cano, Laura, «El derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento (Comentario al artículo 79 RGPD)», en Antonio Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*, Vol. 2, Pamplona: Civitas, 2021, p. 3012.

[13] Véase la situación en otros ordenamientos jurídicos europeos en Moreno Martínez, Juan Antonio, «El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores», en Joaquín Ataz López y José Antonio Cobacho Gómez (coords). *Cuestiones clásicas y actuales del Derecho de daños: estudios en homenaje al profesor Dr. Roca Guillamón*, Vol. 3, Pamplona: Aranzadi, 2021, p. 542 y ss.

[14] El art. 19 de la antigua LOPD de 1999 establecía lo siguiente:

«Derecho a indemnización.

1. 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.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria »

Por tanto, en el ámbito de protección de datos personales, la regla de responsabilidad civil en el ordenamiento jurídico español es la establecida en el art. 82 del RGPD,[15] el cual es directamente aplicable en cada Estado miembro y obligatorio en todos sus elementos (Art. 288 del Tratado de Funcionamiento de la Unión Europea).[16] Así, el art. 82 del RGPD ha reemplazado al antiguo art. 19 de la LOPD como fundamento legal para las pretensiones que se deriven de las infracciones al derecho de protección de datos personales.[17]

Según se mencionó anteriormente, la vigente LOPD no contiene una regla de responsabilidad, a diferencia de su antecesora. Además, el art. 19 de la antigua LOPD establecía una remisión normativa a la legislación reguladora del régimen de responsabilidad patrimonial de las Administraciones públicas. Sin embargo, dicha remisión en la actualidad no existe, de forma tal que surge una pregunta en cuanto a cuál debiese ser la normativa aplicable en el caso de que sea un ente público el responsable del tratamiento de datos personales. Sobre este punto, existe más de una posición al respecto.

Por un lado, existe una parte de la doctrina que indica que se debe aplicar en estos casos la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).[18] En consecuencia, en estos casos la indemnización se exigirá de acuerdo con la LRJSP ante la jurisdicción contencioso-administrativa.[19] A pesar de que la vigente LOPD no contiene una norma como su antecesora (art. 19.2 de la

[15] Art. 82.1. del RGPD indica que «*Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos*».

[16] Plaza Penadés, Javier, «Protección de datos e indemnización por daños en la reciente jurisprudencia del TJUE», en Mariano Herrador Guardia (dir.), *Daño y resarcimiento.* Madrid: Sepin, 2024, p. 398.

[17] Rubí Puig, Antoni, «Daños por infracciones del derecho a la protección de datos personales el remedio indemnizatorio del artículo 82 RGPD», *Revista de Derecho Civil*, vol. V, Nº 4, 2018, p. 57.

[18] Por ejemplo, Plaza Penadés «Protección de datos…», p. 403; Moreno Martínez «El impacto del Reglamento…», p. 552.

[19] López del Moral «Derecho al resarcimiento», p. 3073.

antigua LOPD), estos autores defienden la idea de que, cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá con arreglo a la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

Por otro lado, autores como Busto Lago, indican que se les aplicará directamente el art. 82 del RGPD (norma que establece la responsabilidad civil en el Reglamento[20]), en detrimento de la LRJSP, en sede contencioso-administrativa.[21] El autor argumenta su postura señalando que el art. 4.7 del RGPD incluye expresamente dentro de la definición del responsable del tratamiento a la autoridad pública.[22] Conviene señalar que la antigua LOPD de 1999 mantuvo la distinción que ya estaba en la LORTAD (Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal) sobre la diferenciación entre ficheros de titularidad pública y ficheros de titularidad privada.[23] De acuerdo con Sánchez Bravo, esta distinción que mantuvo la antigua LOPD de 1999 resulta una diferencia con la antigua Directiva de datos personales[24] (que era la normativa aplicable antes de la entrada en vigor del RGPD), la cual tenía como objetivo establecer un régimen igualitario de protección

[20] Véase nota 16.

[21] Esto sería así en virtud del art. 9.4 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y del art. 2.e. de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

[22] Art. 4.7 RGPD. 7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

[23] Artículo 17 apartados 4 y 5 de la LORTAD de 1992:
«4. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.
5. En el caso de los ficheros de titularidad privada la acción se ejercitará ante los órganos de la jurisdicción ordinaria.»

[24] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

centrándose en la figura del responsable del tratamiento, sin importar si la titularidad de los ficheros era pública o privada.[25]

Ante las posiciones descritas, cabe señalar que una de las características de la acción de responsabilidad contenida en el RGPD es que es acumulable con otras.[26] De este modo, sin perjuicio de la existencia de otras acciones (como podría ser la contenida en la LRJSP), en caso de que exista un supuesto que vincule la vulneración de la protección de datos por parte de un responsable que es un ente público, consideramos que es posible presentar acciones en sede contencioso-administrativa basadas en el art. 82 del RGPD.[27]

Sentado lo anterior, para el Derecho catalán resulta importante atender la interpretación que ha dado el Tribunal de Justicia de la Unión Europea (TJUE) de la norma de responsabilidad en cuestión por varios motivos. Primero, porque no existe una norma de responsabilidad en protección de datos en la LOPD, motivo por el cual se aplica directamente el art. 82 del RGPD. Segundo, porque el art. 82 del RGPD es el fundamento legal para ejercer acciones de responsabilidad por infracción de datos personales en el Derecho civil catalán, independiente de la titularidad del fichero o del ejercicio de otras acciones. Tercero, por el carácter vinculante de las sentencias del TJUE. En este sentido, las sentencias del TJUE disponen de interpretaciones que deben orientar el contenido del Derecho civil catalán en el ámbito de la protección de datos personales.

---

25 Sánchez Bravo, Álvaro, «La Ley Orgánica 15/1999, de Protección de datos de carácter personal: diez consideraciones en torno a su contenido», *Revista de estudios políticos*, 2001, Nº 111, p. 207.

26 El carácter acumulable de la acción se basa en lo establecido en el considerando 146 del RGPD («*sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros*»). En el mismo sentido, Rubí Puig, Antoni, «Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección de datos y otras acciones en derecho español», *Revista Derecho Privado y Constitución*, 2019, Nº 34, p. 214.

27 Véase la STSJ Asturias (Contencioso-administrativo, Sección 2ª) de 17 de abril de 2024 (JUR\2024\159131).

3. Algunos aspectos sobre la responsabilidad civil por los daños derivados de una brecha de seguridad

El RGPD establece los principios fundamentales que regulan el derecho a la protección de datos personales. Entre ellos, el art. 82 introduce una norma de responsabilidad civil que merece especial atención. Aunque su redacción parece clara, su aplicación práctica plantea incertidumbres. Esto se debe tanto a la novedad del régimen jurídico como a la escasa regulación existente, lo que da lugar a importantes debates sobre la materia.

Por los motivos expuestos, resulta importante conocer lo que ha sido señalado por el TJUE, órgano que ha interpretado el art. 82 del RGPD a partir de la resolución de cuestiones prejudiciales que han llegado a su conocimiento últimamente. Además, el contenido de estas sentencias es vinculante para los Estados miembros, constituyendo un antecedente de obligatoria observación para el desarrollo del Derecho civil catalán.

Con todo, es preciso advertir que el asunto no se ha caracterizado por su desarrollo. Un ejemplo de esto es que, hasta hace poco, no existían sentencias del TJUE que se refiriesen a la responsabilidad civil en materia de protección de datos.[28] Sin embargo, a fines de 2023 fue resuelta una cuestión prejudicial por el TJUE que precisamente abordó diferentes cuestiones relativas a la responsabilidad civil a causa de una brecha de seguridad producida por un ciberataque de un tercero.[29]

[28] La primera sentencia en la que TJUE se refirió a este asunto fue la STJUE, de 4 de mayo de 2023 (Asunto C-300/21, *RW c. Österreichische Post AG*, ECLI:EU:C:2023:370).

[29] STJUE, de 14 de diciembre de 2023 (Asunto C-340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986). En este caso, la Agencia Nacional de Recaudación búlgara sufrió un ciberataque que generó la publicación en Internet de los datos personales de millones de personas. Un gran número de afectados interpusieron acciones contra la Agencia Nacional de Recaudación, exigiendo un resarcimiento por los daños morales que habían sufrido por el temor a un potencial uso indebido de sus datos personales.

Posterior a esa sentencia, el TJUE se ha manifestado en más de una ocasión sobre el contenido del art. 82 del RGPD.

Como consecuencia de la escasa regulación en la materia, a continuación, se desarrollarán algunas discusiones que se han producido a propósito del alcance y contenido de la norma de responsabilidad del art. 82 del RGPD.

3.1. El criterio de imputación en el RGPD

La doctrina no es uniforme al momento de calificar si la responsabilidad establecida en el art. 82 del RGPD es objetiva o subjetiva.

Una buena parte de la doctrina ha considerado que el criterio de imputación de responsabilidad civil en materia de protección de datos es objetivo, con base en distintos argumentos.[30]

En primer lugar, se destaca el argumento literal: el art. 82.1 del RGPD no menciona expresamente la culpa. Desde esta óptica, se entiende que el legislador europeo, cuando ha querido incorporar criterios culpabilísticos, lo ha hecho explícitamente, como ocurre en el art. 83 del RGPD respecto de la responsabilidad administrativa.[31]

En segundo lugar, el argumento histórico tiene como base el antecedente normativo del RGPD, es decir, la derogada Directiva 95/46/CE que establecía en el art. 23.2 un régimen de responsabilidad

[30] Martín Faba, José María, «Novedades en materia de indemnización y protección de datos personales», *Revista CESCO De Derecho De Consumo*, 2024, Nº49, pp. 145-146; Moreno Martínez «El impacto del Reglamento…», p. 538; Grimalt Servera, Pedro, «Intromisiones ilegítimas en los derechos al honor, a la intimidad y a la propia imagen Tutela civil versus tutela administrativa», Margarita Castilla Barea e Isabel González Pacanowska (coords.), *Protección de datos personales*, Valencia: Tirant Lo Blanch, 2020, p.364; Rubí Puig, «Daños por infracciones…», p. 62.

[31] Grimalt Servera, «Intromisiones…», p. 364.

objetiva.[32] A este respecto, cabe indicar que el considerando 55 de esa Directiva establecía como causas de exoneración aquellas que son propias de la responsabilidad objetiva, a saber: los supuestos de fuerza mayor y los de culpa exclusiva de la víctima.[33] Algunos autores en España sostienen que esas siguen siendo las causas de exoneración en el actual régimen de responsabilidad contenido en el RGPD.[34]

En tercer lugar, es posible justificar un régimen de responsabilidad objetiva a partir de la redacción establecida en el art. 82.3. del RGPD que establece las causas de exoneración de responsabilidad. En efecto, el art. 82.3 en su última parte indica expresamente que el responsable del tratamiento de datos podrá exonerarse «*si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios*». Como se observa, la norma plantea los modos de exoneración desde un punto de vista causal y no de la culpa.[35] Para algún autor, esto refuerza la idea de que la responsabilidad civil no está determinada por el elemento de la culpa o negligencia del responsable del tratamiento de los datos personales.[36]

---

[32] El antiguo art. 23.2 de la derogada Directiva 95/46/CE indicaba 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».

[33] El considerando 55 sostenía en su última parte que «*los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva*».

[34] Por ejemplo, Moreno Martínez «El impacto del Reglamento…», p. 538. En doctrina comparada, véase Van Alsenoy, Brendan, «Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation», *JIPITEC,* 2016, Nº 3, p. 283.

[35] Véase lo señalado por Santos Morón «Reflexiones en torno…», p. 1419.

[36] De Miguel Asensio, Pedro Alberto, «Requisitos del derecho a indemnización en el Reglamento General de Protección de Datos». *La Ley Unión Europea*, 2023, Nº 115, p. 5. En la doctrina comparada, véase Menezes Cordeiro, Antonio, «Civil Liability for Processing of Personal Data in the GDPR». *EDPL*, 2019, Nº. 4, p. 498.

En contraste, otros autores dentro de la doctrina española se han manifestado en el sentido opuesto, es decir, han indicado que el régimen de responsabilidad del RGPD es subjetivo.[37] En rigor, se ha señalado que se está en presencia de un sistema subjetivo de responsabilidad, pero con una inversión de la carga de la prueba de la culpa.

De acuerdo con Busto Lago, quien toma como base el considerando 146 y el art. 82.3 del RGPD, los responsables del tratamiento de datos personales podrán exonerarse de responsabilidad siempre cuando puedan demostrar que el evento dañoso resulta imputable a un hecho ajeno a su esfera de control (como lo puede ser la fuerza mayor o el hecho de un tercero), pero también podrán exonerarse cuando acrediten que han adoptado todas las medidas que son exigidas por las normas y que son técnicamente posibles para evitar que se produzca el daño.[38] Para este autor, la inversión de la carga de la prueba se justifica por los riesgos que comporta una actividad como la de tratamiento de datos.[39]

Esta última posición ha sido la adoptada por el TJUE en sus últimos pronunciamientos sobre la responsabilidad civil en el ámbito de la protección de datos. En este aspecto, el asunto C-667/21 («*Krankenversicherung Nordrhein*») indica expresamente que el art. 82 establece un régimen de responsabilidad por culpa en que la carga de la prueba recae sobre el responsable del tratamiento.[40] Por tanto, se presume la culpa del responsable del tratamiento de datos personales.[41] En esta sentencia, el TJUE ha indicado que un régimen

[37] Busto Lago, José Manuel, «La responsabilidad civil y su función de tutela del derecho a la protección de los datos personales: una visión desde el derecho de la Unión Europea», *Revista Jurídica da UFERSA*,2021. Vol. 5, Nº. 10, p. 33; Nieto Garrido, Eva, «Derecho a indemnización y responsabilidad», José Luis Piñar Mañas (dir.) *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Madrid: Reus, 2016, pp. 561-562.

[38] Busto Lago «La responsabilidad civil…», p. 35.

[39] Busto Lago «La responsabilidad civil…», p. 35.

[40] STJUE, de 21 de diciembre de 2023 (Asunto C-667/21, *Krankenversicherung Nordrhein*, ECLI:EU:C:2024:1051), apartados 94 y 103.

[41] STJUE, *Krankenversicherung Nordrhein* (cit.), apartado 103.

de responsabilidad objetiva no garantizaría la consecución del objetivo de seguridad jurídica perseguida por el legislador y no respetaría el equilibrio entre los intereses de los responsables del tratamiento y los derechos de las personas cuyos datos se tratan.[42]

La doctrina establecida en el asunto C-667/2021, ha sido ratificada por el TJUE en otros asuntos. Así, en los asuntos C-687/21 («*MediaMarktSaturn*»[43]), C-741/21 («*Juris*»[44]) se ha considerado que la culpa se presume, salvo que el responsable demuestre que no es responsable del hecho generador del daño. En otras palabras, se establece un régimen de responsabilidad por culpa con inversión de la carga de la prueba.

Pese a las sentencias citadas, la cuestión dista de estar resuelta. Al respecto, se ha manifestado que lo que se invierte no es la prueba de la culpa, sino que la prueba de la infracción.[45] La inversión de la carga de la prueba es sobre la infracción, pues será el responsable, en función de sus respectivas obligaciones, quien deba acreditar que se han cumplido con las obligaciones contenidas en el RGPD.[46] Además, el propio TJUE presenta inconsistencias en su argumentación. En efecto, en *Juris*, el TJUE, luego de establecer que la responsabilidad era subjetiva con inversión de la prueba de la culpa, se contradice, ya que establece que, en casos de violación de seguridad de los datos personales, el responsable podrá exonerarse si demuestra que no existe una relación de causalidad entre el eventual incumplimiento del RGPD y los daños y perjuicios sufridos por el interesado.[47] Es decir, vuelve a apelar a criterios estrictamente causales y no hace referencia a la prueba de la diligencia para exonerarse de responsabilidad.

---

42 STJUE, *Krankenversicherung Nordrhein* (cit.), apartado 100.

43 STJUE, de 25 de enero de 2024 (Asunto C-687/21, *MediaMarktSaturn,* ECLI:EU:C:2024:72), apartado 52.

44 STJUE, de 11 de abril de 2024 (Asunto C-741/21, *GP contra juris GmbH*, ECLI:EU:C:2024:288), apartado 46.

45 Santos Morón «Reflexiones en torno…», p. 1419.

46 López del Moral «Derecho al resarcimiento», p. 3068.

47 STJUE, *GP contra juris GmbH* (cit.), apartado 51.

También existen posturas intermedias. Santos Morón distingue según se esté en presencia de una obligación de medios o una obligación de resultado en el RGPD. Para esta autora, el criterio de imputación subjetivo con inversión de la carga de la prueba de la infracción se aplicará cuando se trate de una obligación de medios, que exige la apreciación de culpa en el caso concreto. En cambio, en el caso en que la obligación que incumbe al responsable del tratamiento sea una obligación de resultado, en ese caso solamente se podrá exonerar, demostrando que el hecho causante del daño no le es imputable.[48]

En este contexto, será clave conocer los primeros pronunciamientos del Tribunal Supremo sobre la aplicación del RGPD, especialmente en casos donde el responsable sea un ente público. Si se confirma un régimen subjetivo con inversión de la carga de la prueba, será necesario analizar su relación con el sistema objetivo de responsabilidad patrimonial de la Administración.[49]

[48] Santos Morón «Reflexiones en torno…», p. 1421. Es posible encontrar opiniones similares referidas a la antigua LOPD. Al respecto, se ha dicho que «*a la hora de aplicar el artículo 19 LOPD, la Ley no determina si la responsabilidad es objetiva o subjetiva, sin embargo, parece que por norma general lo que habrá que analizar es si el incumplimiento es imputable a un sujeto determinado y si el titular de los datos tiene o no el deber de soportarlo*», en Aberasturi Gorriño, Unai, «El derecho a la indemnización en el artículo 19 de la Ley orgánica de Protección de Datos de Carácter Personal», *Revista Aragonesa de Administración Pública*, 2013, Nº 41-42, p. 191.

También se debe destacar lo señalado por el Abogado General Campos Sánchez-Bordona, dado que, a pesar de dar argumentos que finalmente defienden una responsabilidad objetiva, señala que no cree que el RGPD se ajuste plenamente a ninguno de los dos modelos en puridad. Véase la nota al pie 55 del apartado 72 de las Conclusiones del Abogado General sobre el Asunto C-667/21, presentadas el 25 de mayo de 2023.

[49] Es posible encontrar en alguna sentencia dictada por un tribunal español afirmando que la responsabilidad establecida en el RGPD no es objetiva. Véase SAP Madrid (Sección 20ª), de 28 de junio de 2024 (JUR\2024\308163).

3.2. El principio de seguridad en el RGPD y las brechas de seguridad

3.2.1. El mandato de seguridad en el RGPD

Uno de los principios que inspira el RGPD es el de seguridad. El responsable del tratamiento está obligado a aplicar medidas oportunas y eficaces acordes a las exigencias del RGPD, debiendo estas garantizar un nivel de seguridad adecuado.[50] Así, existe un mandato sobre el responsable de tratamiento de datos personales mediante el cual este debe evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. Como indica el art.5.1.f) del RGPD los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de estos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Por su parte, el art. 4.12 del RGPD define la violación de la seguridad de los datos personales como aquella «*que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*». De acuerdo con el INCIBE, las brechas de seguridad son «*violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos*».[51]

Trasladando la situación al Derecho catalán, en el caso que es objeto de este trabajo, la APDCAT determinó que el HCB no había efectuado un análisis de riesgos necesario para definir las medidas de seguridad aplicables al tratamiento de datos que llevaba a cabo por medio de la plataforma corporativa atacada. En otros términos, el HCB no acreditó haber analizado, en su calidad de responsable, los riesgos que se

[50] Véase tanto los arts. 24 y 32 como los considerandos 74 y 83 del RGPD.

[51] Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

asociaban al tratamiento de los distintos tipos de datos personales que almacenaban en su plataforma.[52]

3.2.2. El alcance de las obligaciones de seguridad

Conviene señalar que no se debe entender este mandato de seguridad que recae sobre los responsables del tratamiento como una responsabilidad a todo evento. En efecto, el TJUE ha señalado que el RGPD exige al responsable del tratamiento a adoptar medidas técnicas y organizativas destinadas a evitar, en la medida de lo posible, cualquier violación de la seguridad de los datos personales.[53] Es decir, el responsable del tratamiento de los datos personales no está obligado a impedir toda violación de seguridad, sino que este debe adoptar las medidas adecuadas para que las violaciones no se produzcan.

El legislador europeo ha entendido que es imposible eliminar todos los riesgos que surgen en la protección de los datos personales, por ese motivo permite al responsable de datos aportar prueba de que las medidas adoptadas eran las apropiadas. El TJUE ha indicado que los jueces de cada Estado miembro deben valorar el carácter apropiado de las medidas técnicas y organizativas, teniendo en cuenta el caso concreto, considerado los riesgos asociados y apreciando la naturaleza, contenido y adopción de esas medidas están adaptados a estos riesgos.[54]

En el procedimiento llevado por la APDCAT, el HCB sostuvo que las medidas adoptadas por este para la protección de los datos personales de sus pacientes eran las adecuadas, pero que era necesario valorar la influencia del nivel de sofisticación de las técnicas intrusivas empleadas por el tercero no autorizado. En otros términos, se apelaba a la idea de que el responsable del tratamiento no puede responder

[52] Véase Resolución sancionadora dictada por la APDCAT, n.º PS 1/2024, de 16 de julio de 2024.

[53] STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), apartado 30.

[54] STJUE, *MediaMarktSaturn* (cit.), apartado 38. Plaza Penades, Javier, «La responsabilidad civil del artículo 82 RGPD en brechas seguridad», *Revista Aranzadi de derecho y nuevas tecnologías*, 2024 Nº 64, p. 4.

ante cualquier caso de vulneración de los datos personales. La defensa del HCB afirma que se está en presencia de obligaciones de medios (donde es necesario observar si el responsable del tratamiento se ha comportado de forma diligente en el cumplimiento de la obligación) y no de resultado (donde se observa si se ha cumplido el mandato establecido en la ley, sin miramientos a la diligencia en el caso concreto).

No obstante, la APDCAT indicó que, si bien las obligaciones de seguridad se configuran como una obligación de medios (y no de resultado),[55] el HCB no había cumplido con el mandato de seguridad de la normativa de protección de datos. En este sentido, la Autoridad establece que el Hospital no había implementado debidamente las medidas que le eran exigibles de acuerdo con el RGPD y tampoco había efectuado el análisis de riesgos pertinente en relación con el tratamiento de datos personales que llevaba a cabo.[56] Por tanto, el HCB no fue diligente en la implementación y aplicación de medidas de seguridad (tanto técnicas como organizativas), de forma tal que estas medidas no eran las apropiadas para garantizar un nivel de seguridad adecuado al riesgo (art. 32 RGPD y art. 28 LOPD).[57]

De este modo, el acceso no autorizado por parte de un tercero o una comunicación no autorizada de datos personales no basta para concluir que las medidas adoptadas por el responsable no eran las adecuadas. No basta con que haya ocurrido un ciberataque para concluir que se está en presencia de un incumplimiento de la obligación de seguridad por parte de responsable. Se deberá valorar, para determinar el carácter apropiado de las medidas, tanto el análisis de riesgos que entrañe el tratamiento como la adecuación de las medidas a los riesgos

[55] Esto también lo ha indicado la jurisprudencia, STS (de lo Contencioso-administrativo) de 15 Febrero de 2022 (RJ\2022\1280).

[56] Véase Resolución sancionadora dictada por la APDCAT, n.º PS 1/2024, de 16 de julio de 2024.

[57] Resolución sancionadora dictada por la APDCAT, n.º PS 1/2024, de 16 de julio de 2024.

teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento.[58]

En virtud de los artículos 5.2, 24.1 y 32.1 del RGPD, la carga de la prueba de que los datos personales se tratan de modo que se garantiza una seguridad adecuada incumbe al responsable de tratamiento.[59] En consecuencia, cuando la infracción tenga relación con la falta de implementación de medidas de seguridad apropiadas, se produce una inversión de la carga de la prueba. Martín Faba justifica esta inversión señalando que los interesados no tienen conocimiento suficiente ni acceso a la información referida a la implementación de las medidas de seguridad que ha adoptado el responsable del tratamiento.[60]

3.3. ¿Qué daños se pueden producir por la brecha de seguridad?

Las violaciones de seguridad de los datos personales pueden llegar a producir daños patrimoniales o extrapatrimoniales para las personas físicas. Cabe advertir que no toda vulneración de seguridad de los datos será motivo suficiente para que proceda la responsabilidad en el caso concreto.[61] En otras palabras, la mera infracción del RGPD no es suficiente para solicitar un resarcimiento.[62] Por tanto, será siempre necesario que el interesado acredite los daños que ha sufrido

[58] STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), apartados 30 y 42. También véase la Resolución sancionadora dictada por la APDCAT, n.º PS 1/2024, de 16 de julio de 2024.

[59] STJUE, *MediaMarktSaturn* (cit.), apartados 42-43; STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), apartados 52 y 57.

[60] Martín Faba «Novedades en…», p.137.

[61] Esto es una diferencia, por ejemplo, con lo regulado en la Ley Orgánica 1/1982, la cual indica en su art. 9.3 que la existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. Es decir, el daño se presume ante la prueba de la infracción a la normativa, cuestión que no ocurre en el ámbito de datos personales.

[62] Véase STS (Civil) de 19 de marzo de 2024 (JUR\2024\92465). En doctrina, Plaza Penadés «Protección de datos…», p.413.

como consecuencia de la vulneración en el tratamiento de sus datos personales.[63]

Como ha sido dicho, el art. 82 del RGPD establece un resarcimiento tanto de los daños patrimoniales como de los extrapatrimoniales a causa de infracciones en el tratamiento de los datos personales. A partir de la amplitud que establece esta cláusula general de daños, conviene preguntarse cuáles son los daños indemnizables y qué criterios se pueden utilizar para distinguir entre aquellos que deben ser resarcidos y los que no en situaciones de brechas de seguridad y que sean útiles para el establecimiento de responsabilidad en el derecho catalán. Concretamente, nos centraremos en dos supuestos.

3.3.1. Daños morales puros

Antes de los primeros pronunciamientos del TJUE en estos asuntos, se consideraba que una brecha de seguridad no era causal suficiente para activar el mecanismo de la responsabilidad civil, sino que servía exclusivamente para notificar a la autoridad competente y a las personas afectadas.[64]

Eso se ha modificado mediante la STJUE del asunto C-340/21 la cual se refiere, entre otras cuestiones, a la aplicación y extensión del artículo 82 del RGPD en este tipo de casos. Concretamente, el TJUE ha considerado que el temor a un potencial uso indebido de datos personales puede constituir por sí solo un daño extrapatrimonial resarcible al amparo del art. 82 del RGPD. Adicionalmente, en varias sentencias posteriores, el TJUE ha reiterado que la mera pérdida

[63] El TJUE lo ha señalado en varias ocasiones, por ejemplo: STJUE, *GP y juris GmbH*, (cit.), apartados 34-35; STJUE, *Österreichische Post AG* (cit.), apartado 42; STJUE, *MediaMarktSaturn* (cit.), apartado 58; STJUE, *Krankenversicherung Nordrhein* (cit.), apartado 82; STJUE, *GP contra juris GmbH* (cit.), apartado 34.

Esto también se observa en sentencias dictadas por tribunales españoles, véase STS (Civil) de 19 de marzo de 2024 (JUR\2024\92465); ATS (Sección 1ª) de 17 de enero de 2019 (JUR\2019\35381); STSJ Andalucía (Sala de lo Social, Sección 1ª) de 10 de enero de 2024 (JUR\2024\104740); SAP Madrid (Sección 20ª), de 28 de junio de 2024 (JUR\2024\308163).

[64] Plaza Penadés «La responsabilidad civil…», p. 1.

de control puede ocasionar una violación de la seguridad de los datos personales que puede causar al interesado daños y perjuicios resarcibles al amparo del art. 82 del RGPD, por mínimos que sean.[65] El TJUE ha sostenido que una vez acreditada una infracción al RGPD, este no distingue entre: (i) los supuestos de daños morales que alega el interesado a causa de un uso indebido de sus datos personales por terceros que ya se ha producido en la fecha de la acción indemnizatoria; (ii) de los supuestos en los que esos daños morales están relacionados con el temor que experimenta ese interesado a que tal uso pueda producirse en el futuro.[66]

En consecuencia, el TJUE ha sido proclive a indemnizar los daños morales puros y ha establecido una regla «*de minimis*» mediante la cual se impone la idea de que no se debe exigir ningún umbral de gravedad de los daños sufridos, siendo estos resarcibles por mínimos que sean. No obstante, es importante destacar que no toda molestia puede considerarse un daño resarcible.[67] Desde esa perspectiva, se deben hacer algunas precisiones que sirvan de orientación para el Derecho civil catalán.

En primer lugar, el RGPD permite una acción por daño moral autónomo, sin que sea necesaria la prueba de algún daño patrimonial.[68] En este sentido, el ordenamiento jurídico español, a diferencia de otros ordenamientos jurídicos europeos, la indemnización del daño moral no es una cuestión que sea objeto de debate.[69]

---

[65] STJUE, *GP contra juris GmbH* (cit.), ap. 42. STJUE, *MediaMarktSaturn* (cit.), ap. 66.

[66] STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), apartado 79.

[67] Santos Morón «Reflexiones en torno…», p. 1414.

[68] Martín Faba «Novedades en…», p. 141; Rubí Puig, «Daños por infracciones…», p. 74.

[69] En cuanto a los diferentes tratamientos que recibe el daño extrapatrimonial en los diversos sistemas jurídicos europeos, véase las reflexiones de Zimmermann, Reinhard, «30. Comparative Report (Categories 11–13) », en Bénédict Winiger et al. (eds.), *Digest of European tort law. Volume 2: Essential Cases on Damages*. Viena: De Gruyter, 2011, pp. 706 y ss.

En segundo lugar, en el ordenamiento jurídico español se reconoce la indemnizabilidad del daño moral puro.[70] Se define como aquel perjuicio «*resultante de la lesión de bienes de la personalidad o de un hecho dañoso cuyas consecuencias se limitan al ámbito puramente moral o espiritual de la víctima*».[71] Como expone Martín Casals, un ejemplo de este tipo de daños es la angustia por el miedo de sufrir un daño que finalmente no se materializa (el caso de «falsos positivos»).[72] Se trata de casos que envuelven únicamente padecimientos emocionales, psíquicos, son daños que derivan de casos de «*perjuicios intangibles y que no acompañan a una pérdida patrimonial, a lesiones personales o a la muerte de la víctima del accidente, son daños reales*».[73]

En tercer lugar, si bien en España se acepta el resarcimiento de distintos supuestos de daños morales, ello no debe conducir a que cualquier menoscabo deba ser indemnizado.[74] Como expone Rubí Puig, resulta cuestionable que cualquier exposición a un riesgo sea

[70] Martín Casals, Miquel, «La «modernización» del derecho de la responsabilidad extracontractual», en Asociación de Profesores de Derecho Civil (Ed.)- *Cuestiones actuales en materia de responsabilidad civil. XV Jornadas de la Asociación de Profesores de Derecho Civil A Coruña, 8 y 9 de abril de 2011*, Murcia: Editum, 2011,p. 119; Martín Casals, Miquel, «Principis per a una proposta de regulació de la responsabilitat extracontractual al Codi Civil de Catalunya», en Institut de Dret privat europeu i comparat de la Universitat de Girona (ed.), *Contractes, responsabilitat extracontractual i altres fonts d'obligacions al Codi civil de Catalunya: materials de les Setzenes Jornades de Dret Català a Tossa*, Girona: Documenta Universitaria, 2012, p. 302; Del Olmo García, Pedro, «Art. 1902», en Ana Cañizares Laso (dir.). *Comentarios al Código Civil. Tomo V.* Primera Edición. Valencia: Tirant Lo Blanch, 2023, p. 8446.

[71] Santos Morón «Reflexiones en torno…», p. 1412.

[72] Martín Casals «La «modernización»…», p. 119; Martín Casals «Principis per…», p. 302.

[73] Gómez Ligüerre, Carlos, «Capítulo I. El concepto de daño moral», en Fernando Gómez Pomar y Ignacio Marín García (Dirs.). *El daño moral y su cuantificación*, 3a ed. Barcelona: Bosch La Ley, 2023, p. 40.

[74] Del Olmo García, Pedro, «Capítulo 2. Epígrafe 1.2. El daño extrapatrimonial», en Ana Soler Presas y Pedro Del Olmo García (coords.). *Practicum Daños*, Cizur Menor: Thomson Reuters, 2019, p. 202.

transformable en un daño moral puro.[75] Siguiendo a Santos Morón, la doctrina «*de minimis*» establecida por el TJUE debería ser entendida en el sentido de que no cabe fijar «*a priori*» un nivel mínimo de gravedad para entender que se está ante un daño indemnizable. Para esta autora, los jueces nacionales de cada Estado miembro, atendiendo las circunstancias concretas, podrán determinar si las consecuencias negativas pueden ser consideradas o no como un daño resarcible.[76]

En cuarto lugar, le corresponderá a la víctima acreditar la existencia de ese daño moral puro. Desde esta perspectiva, el riesgo puramente hipotético no debería dar lugar a indemnización.[77] En palabras de Plaza Penadés, el daño moral debe estar fundado en hechos objetivos y no en meras conjeturas.[78] En el ámbito de protección de datos personales, no existirá *per se* un resarcimiento por vulneración de los datos personales, puesto que ello dependerá de la naturaleza de los datos y las circunstancias concurrentes de cada caso en particular.[79] Es posible encontrar resoluciones en España que han indicado que no basta la mera infracción para imponer la responsabilidad civil, siendo necesario para el interesado acreditar un daño consecuencia de dicha infracción.[80]

En quinto lugar, existe una ausencia de normas comunes que se refieran a la cuantificación de los daños en el Derecho de la Unión

[75] Rubí Puig, Antoni, «Inteligencia artificial y daños indemnizables», en ADPC (eds.), D*erecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Pamplona: Aranzadi, 2024, p. 650.

[76] Santos Morón «Reflexiones en torno…», p. 1414

[77] Martín Faba tiene esta posición respecto al riesgo hipotético de un uso indebido por un tercero. Para este autor, «*el riesgo puramente hipotético de uso indebido podría darse cuando es razonable esperar que ningún tercero ha tenido conocimiento de los datos personales en cuestión. Tampoco parece que se genere daño moral alguno cuando los datos revelados de manera no autorizada son de un tipo cuyo uso indebido es inocuo, como el nombre o la dirección postal*». Véase Martín Faba «Novedades en…», p. 141.

[78] Plaza Penadés «Protección de datos…», p. 422.

[79] Santos Morón «Reflexiones en torno…», p. 1412.

[80] ATS (Sección 1ª) de 17 de enero de 2019 (JUR\2019\35381); STSJ Andalucía (Sala de lo Social, Sección 1ª) de 10 de enero de 2024 (JUR\2024\104740); SAP Madrid (Sección 20ª), de 28 de junio de 2024 (JUR\2024\308163).

Europea, motivo por el cual le corresponde a cada ordenamiento jurídico aplicar sus propias normas referidas a esta materia.[81] En el caso de los daños morales, existe una dificultad para establecer los criterios para cuantificar estos en materias de protección de datos, dada la ausencia de regulación tanto del RGPD como de la LOPD.[82] Al respecto, se pueden observar algunos pronunciamientos por parte del TJUE que pueden servir de orientación al Derecho catalán para cuantificar los daños derivados de una brecha de seguridad. Así, el TJUE ha sostenido que el temor debe estar fundado, habida cuenta las circunstancias del caso y del interesado.[83] En otra de sus últimas sentencias que se refiere a estos asuntos, el TJUE ha indicado que el criterio de que un riesgo meramente hipotético de un uso indebido por un tercero no puede dar lugar a una indemnización, lo cual puede ocurrir cuando ningún tercero ha tenido conocimiento de los datos personales de que se trate.[84] En la doctrina nacional también es posible encontrar autores que se han referido a estas materias. Sobre este punto, Santos Morón ha indicado que el temor debe estar fundado en circunstancias objetivas y no en la opinión subjetiva del interesado.[85] Siguiendo a Rubí Puig, solamente se deberían indemnizar aquellos estados de ansiedad o angustia que estén acreditados medicamente.[86] Adicionalmente, llevando estos criterios al ámbito de protección de datos, se tendría que valorar el tipo de dato personal afectado en el caso concreto, puesto que no es lo mismo un dato relativo a la salud de la víctima —como lo es el caso del HCB— que otro tipo de dato.[87]

[81] STJUE, *GP contra juris GmbH* (cit.), ap. 58. También STJUE *Österreichische Post AG* (cit.), apartado 54; STJUE, *MediaMarktSaturn* (cit.), apartados 47-50; STJUE, *Krankenversicherung Nordrhein* (cit.), apartados 83 y 101.

[82] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[83] STJUE, *VB c. Natsionalna agentsia za prihodite* (cit.), apartado 85.

[84] STJUE, *MediaMarktSaturn* (cit.), ap. 68.

[85] Santos Morón «Reflexiones en torno…», p. 1410.

[86] Rubí Puig, «Daños por infracciones…», p. 76.

[87] Martín Faba «Novedades en…», p. 141.

3.3.2. ¿Un supuesto de «daños preventivos»?

Un supuesto son los posibles daños morales que se pueden derivar de una brecha de seguridad. Las situaciones descritas en el epígrafe anterior deben ser diferenciadas de aquellas situaciones en las cuales el perjudicado, precisamente a causa de los riesgos que se derivan de la brecha de seguridad, ha incurrido en costes destinados a mitigar o evitar daños que amenazan con producirse.

Debe indicarse que varios procesos de reforma de la responsabilidad civil en Europa han centrado su atención en este asunto. La reciente reforma (ya vigente) en Bélgica, dispone una norma que consagra esta figura.[88] También estaba reconocida en los distintos proyectos de reforma en Francia.[89] Conviene señalar que la inspiración de una norma de este tipo se debe a la influencia de los Principios de Derecho Europeo de la Responsabilidad Civil (PETL) y el Marco

[88] El art. 6.28 indica que «*Los gastos resultantes de las medidas urgentes y razonables adoptadas por la parte perjudicada para prevenir un daño inminente o el agravamiento de un daño correrán a cargo de la persona responsable o de la persona que sería responsable si se hubiera producido el daño, incluso si se hubieran realizado sin resultado*». Traducción extraída de Oyarzún Vargas, Felipe, «Acerca del proyecto de reforma de la responsabilidad civil recientemente aprobado en Bélgica», *Anuario De Derecho Civil*, Vol. 77, Nº2, p. 805.

[89] El art. 1237 del Proyecto de reforma de la responsabilidad civil en Francia dispone: «*Los gastos en que incurra el demandante para prevenir la producción inminente de un daño o para evitar su agravación, así como para reducir las consecuencias, constituyen un perjuicio indemnizable si se han efectuado razonablemente*». Traducción en Bergel Sainz de Baranda, Yolanda; Robles Latorre, Pedro (2022). «Traducción del Proyecto de reforma de la responsabilidad civil en Francia». En internet: https://www.henricapitant.org/wp-content/uploads/2022/05/Traduccio%CC%81n-Proyecto-de-Reforma-enero-2022.pdf .

Cabe señalar que este artículo del Proyecto de reforma en Francia tiene como inspiración el art. 1344 del Proyecto Catala, el cual señalaba que «*los gastos expuestos para prevenir la realización inminente de un daño o para evitar su agravación, así como para reducir las consecuencias, constituyen un perjuicio reparable, desde el momento que han sido razonablemente comprometidos*», traducción en Cabanillas Sánchez, Antonio, «El Anteproyecto francés de reforma del Derecho de obligaciones y del Derecho de la prescripción (Estudio preliminar y traducción)», *Anuario de derecho civil*, 2007, Vol. 60, Nº 2, p. 814.

Común de Referencia (DCFR), instrumentos de *soft law* europeo que ya disponían de una norma de tales características.[90]

En general, las disposiciones citadas en el párrafo anterior exigen, para la procedencia de resarcimiento, que se acredite la razonabilidad de los gastos realizados y la inminencia del daño. Si bien en España no se ha caracterizado por el desarrollo de esta tendencia dentro del derecho de daños —a diferencia de lo que ha sido en otros ordenamientos jurídicos comparados[91]—, los supuestos de brecha de seguridad por ciberataques resultan interesantes de cara a estudiar una potencial indemnización por los gastos destinados a imposibilitar un daño en la responsabilidad civil.

4. Conclusiones

1. El incremento de las brechas de seguridad de datos personales subraya la necesidad de estudiar exhaustivamente los diversos aspectos de la responsabilidad civil en este ámbito.
2. En este caso, la jurisdicción competente es la contencioso-administrativa, dado que el HCB es un ente público. En cuanto a la

[90] Por un lado, el art. 2:104 de los PETL «*los gastos realizados para evitar un daño que amenaza producirse constituyen un daño resarcible en la medida en que hayan sido razonables*», traducción en European Group On Tort Law, *Principios de Derecho Europeo de la Responsabilidad Civil*. Cizur Menor: Aranzadi, 2008, p. 26.

Por su parte, la disposición 6:302 del DCFR establece que «*la persona que haya incurrido en unos gastos razonables o haya soportado cualquier otro tipo de daño para impedir la producción de un daño inminente o para limitar el alcance o la gravedad de un daño producido tendrá derecho a ser indemnizada por quien hubiera sido responsable de la causación del mismo*», en Del Olmo García, Pedro; Martín-Casals, Miquel, «Libro VI. Responsabilidad extracontractual. Del capítulo 1 al capítulo 7». En *Principios, definiciones y reglas de un Derecho Civil europeo: el Marco Común de Referencia (DCFR)*, Agencia Estatal Boletín Oficial del Estado, 2015, p. 331.

[91] *V. gr.* en el *Common Law*: Nolan, Donal, «Preventive Damages», *Law Quarterly Review*, 2016, Vol. 132, pp. 68-95; Morgan, Jonathan, *Great Debates in Tort Law*, Oxford: Hart Publishing, 2022, pp. 202-204.

legislación aplicable, consideramos que, por el carácter acumulable de la acción prevista en el art. 82 del RGPD, es posible presentar esta sin perjuicio de la existencia de otras acciones (como la contenida en la LRJSP) en sede contencioso-administrativa.

3. La regulación vigente en materia de responsabilidad civil en el ámbito de la protección de datos personales es insuficiente. Esto genera incertidumbres respecto a la aplicación y el alcance del art.82 del RGPD. Para suplir esta insuficiencia, el Derecho civil catalán se debe orientar por lo que ha sido establecido por el TJUE respecto a la norma de responsabilidad en estos supuestos (art. 82 del RGPD), la cual se debe aplicar con independencia de la titularidad del fichero o del ejercicio de otras acciones.

4. Respecto al criterio de imputación, existe un debate doctrinal sobre si la responsabilidad establecida en el art. 82 del RGPD es objetiva o subjetiva, con una inversión de la carga de la prueba. El TJUE ha adoptado en sus últimas sentencias una postura que defiende la responsabilidad subjetiva con inversión de la carga de la prueba, aunque existen inconsistencias en su argumentación.

5. El RGPD exige a los responsables del tratamiento adoptar medidas técnicas y organizativas adecuadas para evitar violaciones de seguridad, aunque no se les obliga a impedir todas las violaciones. En el caso del HCB, la APDCAT concluyó que este no cumplió con este mandato, al no implementar medidas de seguridad adecuadas ni efectuar el análisis de riesgos pertinente.

6. La mera comisión de una infracción por parte del responsable de tratamiento de datos personales no es suficiente para exigir resarcimiento en materia de datos personales. El interesado debe probar en el juicio los daños que ha sufrido.

7. Las brechas de seguridad pueden causar daños patrimoniales y extrapatrimoniales, incluyendo daños morales puros como el temor a un uso indebido de datos personales.

8. Por más que el TJUE sostenga que no se debe considerar un umbral de gravedad para resarcir los daños, es importante destacar que no toda molestia puede considerarse un daño indemnizable. A pesar de que sea posible mediante el RGPD presentar una demanda de responsabilidad sustentada exclusivamente en daños morales puros (tipo de daño que también se acepta en el ordenamiento jurídico

español), resulta fundamental seguir trabajando los criterios para determinar si es resarcible o no el daño en el caso concreto.

9. La cuantificación de daños en el ámbito de protección de datos es compleja debido a la falta de regulación específica en el RGPD y la LOPD. Se deben atender los criterios que ha ido estableciendo el TJUE y la doctrina nacional sobre este punto.

10. La amplitud de la norma de responsabilidad del RGPD plantea interrogantes acerca de la indemnizabilidad de ciertos supuestos en la responsabilidad civil en estas materias. Uno de ellos podría ser la admisión de los *«gastos preventivos»*, esto es, la admisión del resarcimiento de los costes que ha realizado la víctima o titular de los datos personales para mitigar o evitar daños que amenazan con producirse producto de la brecha de seguridad.

Documenta Universitaria
@DocUniv
documentauniversitaria.com

Universitat de Girona