

Reflexiones en torno a la jurisprudencia del TJUE sobre la acción indemnizatoria del art. 82 RGPD (asuntos C-300/21; C-340/21; C-456/22; C-667/21; C-687/21; C-741/21)

Reflections on the jurisprudence of the CJUE regarding the action for damages under Art. 82 RGPD (cases C-300/21; C-340/21; C-456/22; C-667/21; C-687/21; C-741/21)

MARÍA JOSÉ SANTOS MORÓN
Catedrática de Derecho civil,
Universidad Carlos III de Madrid
ORCID: 0000-0001-6486-4869

Recibido: 16.05.2024 / Aceptado: 04.07.2024

DOI: 10.20318/cdt.2024.8983

Resumen: El propósito de este trabajo es poner de manifiesto las interrogantes que suscita la reciente jurisprudencia del TJUE en torno el art. 82 RGPD. Aunque teóricamente las sentencias analizadas vienen a “aclarar” el sentido de dicho precepto, en algunos aspectos resultan poco esclarecedoras, bien arrojando nuevas dudas, bien realizando planteamientos confusos en torno a elementos claves de la responsabilidad.

Palabras clave: Protección de datos personales, infracción, daño, carga de la prueba, culpabilidad, relación causal, causas de exoneración.

Abstract: The purpose of this paper is to address the issues raised by the recent case law of the CJEU on Art. 82 GDPR. Although in theory the judgments analysed are intended to “clarify” the meaning of this provision, in some aspects they are not very enlightening, either by raising new doubts or by adopting confusing approaches to key elements of liability.

Keywords: Personal data protection, infringement, damage, burden of proof, fault, causal link, exoneration causes.

Sumario: I. Introducción. II. Sobre el daño indemnizable en las demandas basadas en el art. 82 RGPD. A) Para que exista deber de indemnizar es necesaria la prueba del daño. El resarcimiento del daño inmaterial no requiere un umbral mínimo de gravedad. B) El temor al uso indebido de los datos, o la pérdida de control de éstos puede constituir daño inmaterial, pero es preciso probarlo. C) El temor al mal uso de los datos debe estar justificado para que sea objeto de resarcimiento. El art. 82 RGPD tiene función indemnizatoria. D) ¿Puede o no tomarse en consideración la gravedad de las consecuencias negativas sufridas por el afectado para determinar que existe daño inmaterial? E) ¿Cuándo, entonces, estamos ante un daño inmaterial o moral?. III. Sobre el criterio de imputación de la responsabilidad y los requisitos para que exista una infracción que dé lugar a responsabilidad. A) No toda vulneración de la seguridad de los datos constituye una infracción. B) ¿Responsabilidad objetiva o por culpa? Causas de exoneración de responsabilidad. C) La necesidad de distinguir entre los requisitos para que exista una infracción y los requisitos para que exista responsabilidad. IV. Conclusiones.

Introducción¹

1. El art. 82 RGPD (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 abril 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, DOUE L 119 de 4 de julio), como ya establecía el art. 23 de la Directiva 95/46,² consagra la posibilidad de ejercitar acciones de responsabilidad dirigidas a obtener la reparación de los daños que haya podido producir la infracción de la normativa de protección de datos personales. La acción de responsabilidad, que deberá plantearse ante los tribunales competentes conforme a la legislación interna del Estado de que se trate (art. 82,6)³, puede ejercitarse frente al responsable del tratamiento o frente al encargado⁴, si bien en este segundo caso, solo cuando el encargado del tratamiento “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”⁵. Por ello en la práctica lo más frecuente es que la demanda se entable frente al responsable del tratamiento quien, de acuerdo con el art. 24 RGPD, tiene el deber de garantizar que el tratamiento es conforme con el RGPD y, como se deduce del Cdo. 146 RGPD, también con la normativa interna que lo concrete o desarrolle⁶.

2. La interpretación del art. 82 RGPD suscita, sin embargo, no pocas dudas, y así lo ponen de manifiesto las numerosas cuestiones prejudiciales planteadas por tribunales de distintos países (sobre todo alemanes) que han dado lugar en los últimos meses a varias sentencias del TJUE.

Concretamente, las sentencias que se van a analizar (SSTJUE 4 mayo 2023, *Österreichische Post*, C-300/21, EU:C:2023:370; 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986; 14 diciembre 2023, *Gemeinde Ummendorf*, C-456/22, EU:C:2023:988; 21 diciembre 2023, *Krankenversicherung Nordrhein*, C-667/21, EU:C:2023:1022; 25 enero 2024, *MediaMarktSaturn*, C-687/21, EU:C:2024:72; 11 abril 2024, *Iuris*, C-741/21, EU:C:2024:288) resuelven diversas cuestiones, relacionadas con: a) los requisitos para que exista una infracción de la normativa de protec-

¹ Este trabajo se ha realizado en el marco del Proyecto de Investigación PID2020-115352GB-I00, financiado por AEI/10.13039/501100011033.

² Directiva 95/46 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 esos datos, DOCE L 281, de 23 noviembre 1995.

³ El art. 86,2 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). Si la víctima del daño ejercita su acción ante tribunales españoles, deberá hacerlo ante 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.

⁴ Sobre los conceptos de responsable y encargado del tratamiento, vid. SANTOS MORÓN, “Tratamiento de datos, sujetos implicados, responsabilidad proactiva”, en *Protección de Datos Personales*, APDC, Tirant lo Blanch, Valencia, 2020, pp. 35 y ss.; 45 y ss.

⁵ Conviene advertir que 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. Es decir, el responsable del tratamiento no puede liberarse de responsabilidad aduciendo que el comportamiento infractor ha sido cometido por el encargado del tratamiento (RUBÍ PUIG, “Daños por infracción del derecho a la protección de datos personales, El remedio indemnizatorio del art. 82 RGPD”, *RDC*, 2018, vol. V, nº 4, p. 46; HERRÁN ORTIZ, “El responsable y el encargado del tratamiento de datos personales: a propósito de un nuevo régimen de responsabilidad en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018, de 5 de diciembre”, en *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al prof. Dr. Roca Guillamón*, t. III, Thomson Aranzadi, Navarra, 2021, p. 1450). Además, en los casos en que pueda existir responsabilidad del encargado el responsable del tratamiento responderá solidariamente junto con él (art. 82,4 RGPD, art. 30,2 LOPD).

⁶ El Cdo. 146 RGP 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”.

ción de datos, b) el criterio de imputación de la responsabilidad ex art. 82 RGPD, c) el daño indemnizable, d) la carga de la prueba y e) la función -indemnizatoria o punitiva- del citado art. 82.

3. La mayoría de las resoluciones se pronuncian sobre varias de estas cuestiones, que suelen estar estrechamente imbricadas, recogiendo, en su caso, el criterio sentado para cada una de ellas en sentencias anteriores. No obstante, el TJUE ofrece razonamientos que arrojan nuevos interrogantes, en mi opinión no adecuadamente resueltos, o que pueden resultar confusos en la medida que no diferencian adecuadamente conceptos distintos como la infracción, la culpa o la causalidad.

A continuación, vamos a examinar conjuntamente el contenido de estas sentencias diferenciando dos bloques temáticos relativos, respectivamente, al daño indemnizable, y al criterio de imputación de responsabilidad.

II. Sobre el daño indemnizable en las demandas basadas en el art. 82 RGPD.

4. Son varios los tribunales de Estados miembros que han planteado cuestiones prejudiciales relativas a la necesidad o no de que exista daño indemnizable y, en su caso, la naturaleza de éste. En primer lugar se cuestiona si, para que exista deber de indemnizar, basta con que se cometa una infracción de la normativa de protección de datos o es necesario además que exista un daño, circunstancia esta que está en cierta medida relacionada con otra de las dudas planteadas, relativa a si el art. 82 RGPD tiene carácter punitivo y no meramente indemnizatorio (pues en tal caso parece evidente que bastaría la existencia de la infracción, no siendo necesaria la existencia de un daño objeto de reparación). Pero el principal problema es quizás, una vez constatada la necesidad de que se produzca un daño, qué debe entenderse por “daño inmaterial” –pues el art. 82,1 RGPD permite la indemnización tanto del daño “material” como “inmaterial”-, interrogante que se plantea en varias de las sentencias examinadas y que, a mi juicio, el TJUE no resuelve claramente. Veámoslo a continuación.

A) Para que exista deber de indemnizar es necesaria la prueba del daño. El resarcimiento del daño inmaterial no requiere un umbral mínimo de gravedad.

5. En el supuesto que dio lugar a la STJUE 4 mayo 2023, *Österreichische Post*, C-300/21, la primera que aborda el tema de los requisitos para que exista derecho a indemnización ex art. 82 RGPD, una sociedad austriaca dedicada a la venta de direcciones trató datos de numerosos sujetos para, con ayuda de un algoritmo y mediante extrapolación estadística, inferir afinidades políticas con vistas al envío de publicidad electoral⁷. El demandante del litigio principal, que no había dado su consentimiento para el tratamiento de sus datos personales, se sintió ofendido porque se le vinculó con cierto partido político y, aunque esos datos no se transfirieron a terceros, presentó una demanda solicitando el cese del tratamiento y una indemnización por los daños inmateriales sufridos. Desestimada la demanda indemnizatoria en las instancias inferiores, el Tribunal Supremo de lo Civil y Penal austriaco cuestiona: i) si el reconocimiento del derecho a indemnización exige que el demandante haya sufrido daños y perjuicios o basta la infracción del RGPD; ii) si existen requisitos específicos en el Derecho de la Unión para cuantificar tal indemnización y iii) si es compatible con el Derecho de la Unión la exigencia de que exista una consecuencia o secuela de cierta gravedad para reconocer perjuicios inmateriales.

6. El TJUE responde a las mencionadas cuestiones prejudiciales afirmando, en primer lugar, que no basta la existencia de una infracción del RGPD para reconocer derecho a indemnización ya que el art. 82 exige tres requisitos cumulativos: la existencia de una infracción, la existencia de daño y la relación

⁷ Comentan esta sentencia DE MIGUEL ASENSIO, “Requisitos del derecho a indemnización en el Reglamento General de Protección de Datos”, *La Ley Unión Europea*, nº 121, 2024; PLAZA PENADÉS, “Protección de datos e indemnización por daños en la reciente jurisprudencia del TJUE”, en *Daño y resarcimiento*, Sepin, Madrid, 2024, pp. 411, 414.

de causalidad entre una. De los Cdos. 75, 85 y 146, se deduce, además, que la producción de daños y perjuicios como consecuencia de una violación del RGPD es solo potencial, de manera que *la infracción de dicha norma no conlleva necesariamente daños y perjuicios* (ap. 32-37).

7. Presuponiendo, por tanto, que ha de existir un daño, observa que el concepto de daños y perjuicios debe interpretarse en sentido amplio, según se desprende del Cdo. 146 RGPD, lo cual es necesario (Cdo. 10, para garantizar un nivel uniforme y elevado de protección en lo que respecta al tratamiento de datos personales (ap. 46-48)

Dado que el art. 83 RGPD se limita a enunciar que pueden dar derecho a indemnización tanto los daños materiales como los inmateriales, sin mencionar ningún umbral de gravedad, concluye afirmando que el citado precepto se opone a una norma o práctica nacional que supedita la indemnización por daños inmateriales al requisito de que alcancen cierta gravedad. Ahora bien, esto no significa que el afectado no tenga que demostrar que las *consecuencias negativas* derivadas de la infracción *constituyen daños y perjuicios inmateriales* (vid. ap. 50,51).

8. Por último, en relación con la cuantificación de la indemnización, el TJUE indica que, dado que el RGPD no contiene ninguna disposición al respecto, corresponde al ordenamiento interno de cada Estado establecer los criterios para determinarla, siempre que se respeten los principios de equivalencia y efectividad (ap. 54), lo que implica que la indemnización de que se trate debe compensar íntegramente los daños y perjuicios sufridos como consecuencia de la infracción (ap. 57,58).

B) El temor al uso indebido de los datos, o la pérdida de control de éstos *puede* constituir daño inmaterial, pero es preciso probarlo.

9. La doctrina vertida en esta sentencia es reiterada en resoluciones posteriores. En la STJUE 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, en la que, a raíz de un ciberataque al sistema informático de un organismo búlgaro se publicaron en internet datos personales de ciertos sujetos, el TJUE responde a la quinta cuestión planteada por el órgano remitente -que indagaba si puede considerarse el mero temor al uso indebido de los datos personales como un daño inmaterial *aunque no se constate ningún otro perjuicio*- recordando lo expresado en la sentencia anteriormente comentada (vid. ap. 77, 78)⁸.

10. A partir de ahí, observa que el art. 82 no distingue según que los daños inmateriales estén relacionados con un uso indebido de los datos ya producidos o con el temor de que se produzcan en el futuro. Reitera lo indicado en la citada STJUE 4 mayo 2023 sobre la necesidad de interpretar ampliamente el concepto de daños y argumenta que, del Cdo. 85, se deduce que el legislador europeo quiso incluir en los conceptos constitutivos de daños la *“mera pérdida de control”* aunque no se haya producido un uso indebido de los datos en cuestión (ap. 79-82). Por ello concluye que el temor de una persona a un uso indebido de sus datos por terceros *“puede constituir, por sí solo, un daño o perjuicio inmaterial”* a efectos del art. 82 RGPD (ap. 86).

11. Ahora bien, aunque ello es así, el TJUE subraya –repetiendo lo afirmado en la sentencia anteriormente mencionada- que el interesado *“que haya tenido consecuencias negativas para él debe demostrar que estas consecuencias constituyen daños y perjuicios inmateriales”* (ap. 84) y añade que, en el supuesto concreto de temor al uso indebido de los datos personales, *“el órgano jurisdiccional que conozca el asunto deberá comprobar que ese temor puede considerarse fundado”* atendiendo a las circunstancias concretas (ap. 85).

⁸ Sobre esta sentencia vid. PLAZA PENADÉS, ob. cit., pp. 414 y ss.; MARTÍN FABA, “Novedades en materia de indemnización y protección de datos personales”, *Revista Cesco de Derecho de Consumo*, nº 49/2024, pp. 133 ss

12. Un problema similar dilucida la STJUE 14 diciembre 2023, *Gemeinde Ummendorf*, C-456/22. En este caso el ayuntamiento de una localidad alemana, al publicar en internet el orden del día de una sesión del consejo municipal, divulgó datos personales de los demandantes, que adujeron que se había producido una difusión ilícita de sus datos que les había causado un daño inmaterial. El órgano remitente, en la única cuestión prejudicial planteada en este asunto, pregunta si el concepto de daño inmaterial exige un perjuicio tangible o basta con que el interesado se haya visto privado temporalmente del poder de disposición sobre sus datos por un periodo de pocos días, *sin que de ello se hayan derivado consecuencias tangibles o perjudiciales de ningún tipo*.

13. El tribunal europeo, remitiéndose a la doctrina sentada en la S. 4 mayo 2023, *Österreichische Post*, C-300/21, reiterada por la de 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, afirma que, no siendo exigible un umbral mínimo de gravedad para que el daño inmaterial sea objeto de indemnización, tampoco puede exigirse el carácter tangible del daño o la naturaleza objetiva del perjuicio (ap. 17, 18). Concluye diciendo, por tanto, que nada se opone a que la pérdida de control de los datos durante un breve periodo de tiempo *pueda* causar a los interesados daños y perjuicios inmateriales. Ahora bien, sigue siendo necesario que dichos interesados *“demuestren que han sufrido efectivamente tales perjuicios, por mínimos que sean”*. Es decir, el interesado que haya tenido consecuencias negativas debe demostrar que estas consecuencias constituyen daños inmateriales en el sentido del art. 82 (ap. 21, 22).

14. La interrogante que surge a raíz de estas sentencias es que, si la pérdida temporal del control de los datos o el temor a que sean mal utilizados *puede* constituir daño inmaterial, pero el interesado *debe demostrar* que las consecuencias negativas sufridas efectivamente constituyen daño inmaterial, sin que pueda tomarse en consideración la *gravedad* de dichas consecuencias ¿qué criterios cabe usar para concluir que efectivamente se está ante un daño “inmaterial”? En realidad, el TJUE no resuelve en absoluto la cuestión planteada, pues, incurriendo en una clara tautología, viene a decir que *la situación alegada por el demandante puede constituir daño inmaterial cuando se pruebe que es daño inmaterial*.

15. El razonamiento se repite, desafortunadamente, en algunas otras de las sentencias examinadas, aunque la STJUE 25 enero 2024, *MediaMarktSaturn*, C-687/21, añade una matización de cierta utilidad.

C) El temor al mal uso de los datos debe estar justificado para que sea objeto de resarcimiento. El art. 82 RGPD tiene función indemnizatoria.

16. En la mencionada resolución (STJUE 25 enero 2024, *MediaMarktSaturn*, C-687/21) relativa a un supuesto en que el empleado de una empresa entregó, por error, un documento con datos personales del demandante a otro cliente⁹, el tribunal alemán remitente, además de plantear nuevamente la duda sobre si la mera existencia de una infracción justifica el deber de indemnizar, pregunta: i) si el art. 82 RGPD tiene función punitiva, y, ii) en relación nuevamente con el concepto de daño, si la entrega a un tercero de un documento con datos personales ajenos puede dar lugar a un daño inmaterial aunque el tercero parezca no haber tenido conocimiento de dichos datos (cuestiones prejudiciales 2^a, 6^o y 7^o).

17. Respecto de la primera cuestión enunciada, el TJUE, como no podía ser menos, reitera las afirmaciones de la S. 4 mayo 2023, *Österreichische Post*, C-300/21, en torno a la necesidad de que exista, además de una infracción, un daño relacionado causalmente con la misma (ap. 56-61). Sobre el carác-

⁹ El demandante del litigio principal compró un aparato eléctrico a cierta empresa con financiación, para cuya obtención debía suscribir un documento que contenía datos personales suyos. Dicho documento, sin embargo, fue entregado por error por un empleado de la compañía a otro cliente. El error fue advertido por dicho empleado casi inmediatamente, recuperando los documentos en un plazo de una media hora, sin que el tercero hubiera llegado a ser consciente de que se le había facilitado información personal de otro cliente

ter punitivo o indemnizatorio del art. 8 RGD, sostiene que dicho precepto -como ya había establecido en una sentencia anterior, de 21 diciembre 2023, *Krankenversicherung Nordrhein*, C-667/21¹⁰- tiene función compensatoria, por lo que la gravedad de la posible infracción no influye en la cuantía de la indemnización, que no puede superar la extensión del perjuicio sufrido (ap. 46-50). Y, respecto a la noción de perjuicio inmaterial, recuerda que el temor a un posible mal uso de los datos o le pérdida de control de los mismos, aun por corto periodo, pueden constituir daño inmaterial, pero “*sujeto a la demostración por parte del afectado de que efectivamente ha sufrido tal daño, aunque sea mínimo*” (ap. 65, 66).

18. Aunque esta resolución reitera el razonamiento de las sentencias anteriores, introduce un matiz clarificador. Así, tras afirmar que una situación en la que el titular de los datos experimenta un miedo *bien fundado*¹¹, a valorar por el juez nacional, de que sus datos sean difundidos o mal usados por terceros en el futuro encaja en el concepto de daño inmaterial (ap. 67), advierte que “*el puro hipotético riesgo de mal uso por parte de un tercero no autorizado no puede dar derecho a indemnización*” (ap. 68). Aplicando esta idea al caso concreto -en que el tercero al que se le facilitó un documento con los datos personales del afectado no llegó a ser consciente de ello- sostiene que no existe daño inmaterial por el mero hecho de que el interesado tema que, habiendo sido posible que el tercero hiciera una copia del documento en cuestión, pueda producirse su divulgación o mal uso en el futuro (ap. 69).

19. La conclusión que de ello cabe extraer es que, para que el temor al mal uso de los datos cuyo control se ha perdido transitoriamente pueda constituir daño moral, es necesario que dicho temor esté fundado en circunstancias objetivas y no en la opinión subjetiva del interesado.

D) ¿Puede o no tomarse en consideración la gravedad de las consecuencias negativas sufridas por el afectado para determinar que existe daño inmaterial?

20. Por último, en la S. 11 abril 2024, *Juris*, C-741/21, el TJUE vuelve, otra vez, sobre el concepto de daño inmaterial. En este caso, el demandante del litigio principal, cliente de una base de datos de carácter jurídico, se opuso a que dicha empresa tratara sus datos con fines de mercadotecnia directa, pese a lo cual recibió en varias ocasiones publicidad, lo que le llevó a reiterar su oposición y demandar, finalmente, a la empresa mencionada, exigiendo indemnización por daños materiales (gastos judiciales y notariales) e inmateriales. El órgano remitente -un tribunal alemán- planteó diversas cuestiones prejudiciales relativas, por lo que en este punto nos interesa, a: i) si el concepto de daño inmaterial comprende cualquier menoscabo de la posición jurídica protegida -tégase en cuenta que aquí se había vulnerado repetidamente el derecho de oposición del afectado- con independencia de sus efectos y su relevancia; ii) si cabe recurrir a los criterios establecidos en el art. 83 RGD, relativo a multas administrativas, para calcular el importe de la indemnización por daños inmateriales y iii) si debe existir una indemnización por cada infracción o pueden “sancionarse” (sic.) varias con una indemnización global (cuestiones 1ª, 3ª y 4ª).

21. El TJUE responde conjuntamente a la tercera y cuarta cuestión prejudicial, reiterando que la función del art. 82 RGD no es punitiva, por lo que no pueden tomarse en consideración los criterios

¹⁰ En el asunto que dio lugar a esta sentencia un organismo público alemán que emitía informes médicos sobre la capacidad laboral de personas aseguradas en la Caja de seguro obligatorio de enfermedad, emitió un informe médico sobre uno de sus empleados, a raíz de su situación de incapacidad laboral. El afectado consideraba que se había llevado a cabo un tratamiento ilícito de sus datos de salud. En este caso las cuestiones planteadas por el órgano remitente se refieren a la interpretación de los arts. 9 y 6 del Reglamento (cuestiones 1 a 3), la necesidad de que exista culpa para imponer responsabilidad (cuestión 5) y, por lo que ahora interesa, a si la función del art. 82 es preventivo/punitiva, debiendo tenerse en cuenta ese posible carácter para fijar el importe de la indemnización (cuestión 4). El TJUE respondió a esta última cuestión afirmando que el art. 82 RGD no tiene función punitiva, siendo su función, según se deduce del Cdo. 146, y a diferencia de lo que se desprende de otros preceptos como el art. 83 y 84 RGD, la reparación íntegra del daño. Por consiguiente, la gravedad de la infracción no puede incidir en la cuantía de la indemnización (vid. ap.84-87).

¹¹ Advértase que la necesidad de que el miedo al mal uso de los datos esté fundado, ya fue establecida en la S. STJUE 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, aunque quizás, con menos relevancia.

establecidos en el art. 83 para las multas administrativas en la cuantificación de la indemnización, y afirmando que el hecho de que se hayan cometido varias infracciones no es un criterio pertinente para fijar su importe, ya que a tal efecto solo deben tenerse en cuenta los perjuicios sufridos por el interesado¹².

22. Respecto de la primera cuestión prejudicial, que es la que más nos interesa, el TJUE comienza recogiendo lo ya mantenido en sentencias anteriores y reitera que la persona que reclama una indemnización debe probar que la infracción le ha causado daños y perjuicios, aunque dicha indemnización no está supeditada a que los mismos hayan alcanzado cierta gravedad (ap. 34-36).

23. En relación con el caso concreto afirma que la infracción de disposiciones del RGPD que otorgan derechos al interesado *no puede por sí sola fundamentar el derecho a obtener una indemnización*, ya que debe existir daño y relación causal. Ahora bien, como el demandante del litigio principal basaba su derecho a indemnización en la pérdida de control de los datos, el TJUE recuerda que en sentencias previas ya había afirmado que tal pérdida de control puede causar al interesado daños inmateriales, “siempre que dicho interesado *demuestre que ha sufrido efectivamente tales daños y perjuicios, por mínimos que sean*” (ap. 40-42). Aplicando este criterio al caso enjuiciado concluye afirmando que “una infracción de disposiciones de este Reglamento que confieren derechos al interesado no puede constituir, por sí sola, un supuesto de «daños y perjuicios inmateriales» a efectos de dicha disposición, *con independencia de la gravedad de los daños y perjuicios sufridos por ese interesado*” (ap. 43).

24. Lo expresado por el TJUE en el último párrafo citado –que reitera en sus conclusiones, ap. 66- resulta un tanto llamativo pues, pese a haber manifestado en párrafos anteriores, de acuerdo con lo mantenido en resoluciones previas, que no cabe supeditar el derecho a indemnización a la exigencia de que los daños no patrimoniales alcancen cierta gravedad (vid. ap. 36), concluye afirmando, en clara contradicción con tal declaración, que la vulneración de los derechos conferidos por el RGPD al interesado no constituye por sí sola un perjuicio inmaterial “*con independencia de la gravedad*” del concreto daño sufrido por éste.

25. ¿Está diciendo el TJUE, en definitiva, que para entender que la violación de los derechos conferidos por el RGPD al afectado constituye un daño inmaterial *sí es relevante la gravedad de los perjuicios* –distintos a la mera vulneración del derecho de que se trate- que puedan derivarse de tal infracción?¹³

26. Como decía al principio, me parece que las resoluciones analizadas arrojan, en algunos aspectos, más dudas que certezas.

E) ¿Cuándo, entonces, estamos ante un daño inmaterial o moral?

27. En relación con las conclusiones extraídas de las sentencias comentadas, cabe hacer las siguientes consideraciones:

¹² A tal afirmación cabría, no obstante, objetar que, si se han infringido repetidamente los derechos del interesado, lo lógico es pensar que la extensión del daño será mayor, por lo que, en consecuencia, la indemnización también lo será.

¹³ Para intentar salir de dudas se han consultado otras versiones lingüísticas de la sentencia comentada (concretamente la inglesa y la francesa), pero se pronuncian en el mismo sentido que la española. En la versión inglesa el apartado 43 dice lo siguiente: “In the light of the foregoing reasons, the answer to the first question is that Article 82(1) of the GDPR must be interpreted as meaning that *an infringement* of provisions of that regulation which confer rights on the data subject *is not sufficient*, in itself, to constitute ‘non-material damage’ within the meaning of that provision, *irrespective of the degree of seriousness of the damage suffered by that person*”. El texto de la versión francesa reza como sigue: “Compte tenu des motifs qui précèdent, il y a lieu de répondre à la première question que l’article 82, paragraphe 1, du RGPD doit être interprété en ce sens qu’*une violation* de dispositions de ce règlement qui confèrent des droits à la personne concernée *ne suffit pas, à elle seule*, pour constituer un «dommage moral», au sens de cette disposition, *indépendamment du degré de gravité du préjudice subi par cette personne*”.

- 1º) El TJUE ha afirmado que, para que exista deber de indemnizar, no basta la existencia de una infracción del RGPD, siendo necesario que se pruebe que ésta ha causado daños. La necesidad de que se produzca un daño es, en realidad, obvia, puesto que se trata de un elemento indispensable de toda acción de responsabilidad, sea contractual o extracontractual. Lo que no es tan obvio, y de ahí la relevancia de lo aclarado por el tribunal europeo, es que toda infracción de la normativa de protección de datos pueda provocar perjuicios. Muchos de los deberes que el RGPD impone al responsable (o, en su caso, encargado) del tratamiento están dirigidos a garantizar que se respetan los principios del tratamiento y los derechos del perjudicado. Sin embargo, también hay normas que tienen un carácter puramente instrumental o se establecen frente a la autoridad de control. Piénsese, por ej., en 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 del responsable del tratamiento de disponer de un registro de actividades (art. 30 RGPD), 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). Parece evidente que el incumplimiento de estos deberes por parte del responsable del tratamiento, aun constituyendo una infracción de la normativa de protección de datos¹⁴, no tiene por qué provocar perjuicios a personas concretas, en cuyo caso, como es lógico, no podrán pedir indemnización.
- 2º) El daño, que ha de ser probado por el interesado, puede ser, según el art. 82 RGPD, material o inmaterial -o, según la terminología preferible desde la perspectiva del Derecho español-patrimonial o no patrimonial (daño moral)¹⁵. La prueba del daño patrimonial, en principio, no presenta dificultades, pero la situación no es igual cuando se trata del daño moral. Hay casos en los que la vulneración de la normativa de protección de datos puede provocar, a su vez, una intromisión en el derecho al honor o en la intimidad del perjudicado¹⁶. En tal hipótesis, por lo que respecta a nuestro ordenamiento, deberá presumirse la existencia de un daño moral por aplicación del art. 9,3 LO 1/82 de Protección al Honor, la intimidad y la imagen. Ahora bien, no toda infracción causa a su vez una lesión en estos derechos. Ni siquiera el acceso indebido a datos personales supone necesariamente una vulneración de la intimidad de la persona a que se refieren, pues ello dependerá de la naturaleza de los datos y las circunstancias concurrentes¹⁷. Por tanto, fuera de los supuestos de vulneración de otros

¹⁴ En España, todos estos comportamientos están catalogados en la LOPD (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales) como infracciones administrativas susceptibles de ser sancionadas.

¹⁵ El daño suele calificarse como patrimonial o extrapatrimonial en función de los intereses afectados. No obstante, dentro del daño extrapatrimonial suele distinguirse el daño moral derivado de lesiones a la integridad personal o la muerte de un sujeto (daño corporal) y el daño moral puro, que es el 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 (v. gr. sufrimiento psíquico y moral consecuencia del vaciado por error de un nicho y traslado de los restos a una fosa común; miedo a morir ahogado a consecuencia de un naufragio, etc.) (DEL OLMO, “El daño extrapatrimonial”, en *Practicum Daños 2019*, Thomson Reuters, Navarra, 2019, pp. 199-201, 203; GÓMEZ LIGÜERRE, “Concepto de Daño moral”, en GÓMEZ POMAR/MARÍN GARCÍA, *El daño moral y su cuantificación*, Wolter Kluwer, Barcelona, 2015, p. 37, 39, 51, 53). Como observa DEL OLMO (ob. cit., p. 202) llamar daño “inmaterial”, por ej., al derivado de una pierna escayolada resulta “contraintuitivo”, del mismo modo que tampoco parece convincente llamar daño “material” al lucro cesante. En cualquier caso, en el supuesto de vulneración al derecho de protección de datos estaremos ante el denominado daño moral puro, derivado de la lesión de un bien inmaterial.

¹⁶ Ejemplo de lo primero son los casos de inclusión indebida de una persona en un fichero de morosos. También puede provocar una lesión en el derecho al honor o la intimidad del afectado la no satisfacción de su derecho al olvido (cfr. STS, Sala 1ª, 15 octubre 2014 –ECLI:ES:TS:2015:4132-; STS, Sala 1ª, 5 abril 2015 –ECLI:ES:TS:2016:1280-). Vid. RUBÍ PUIG, ob. cit., p. 75; BUSTO LAGO, “Protección de datos personales y responsabilidad civil”, *Derecho de daños 2020*, Lefebvre, 2020, pp. 496, 497 ss.; SANTOS MORÓN, “La responsabilidad por incumplimiento de la normativa de datos personales”, en VENDRELL/GSELL/KINDL, *Die Schadenersatzhaftung, La responsabilidad civil*, Nomos, 2022, pp. 246, 247.

¹⁷ Así lo afirma la reciente STS, Sala 1ª, 19 marzo 2024 (ECLI:ES:TS:2024:1495). Una empleada de una empresa, utilizando indebidamente la clave de ésta, realizó una consulta de datos de solvencia de su hermano y sobrina en un fichero de morosos (ASNEF). Estos presentaron una demanda aduciendo, entre otras cosas, que se había vulnerado su derecho a la intimidad. El TS, tras afirmar que no todo acceso a datos protegidos constituye una violación del derecho a la intimidad, afirma que en la

derechos de la personalidad ¿cuándo cabe entender que la infracción de la normativa de protección de datos genera un daño moral?

- 3º) Como es sabido en el Derecho español –a diferencia de lo que sucede en otros ordenamientos- se admite con gran amplitud la posibilidad de indemnizar el daño moral¹⁸. Dado que el TC ha definido el derecho a la protección de datos como un derecho fundamental que atribuye a las personas físicas “el poder de disposición sobre sus propios datos, sean o no íntimos” (STC 292/2000 de 30 de noviembre; 160/2021 de 4 de octubre) cabría pensar que, si se tratan ilícitamente los datos personales de un sujeto de modo que este pierde su control, o se vulneran los derechos del perjudicado (acceso, rectificación, oposición, cancelación), existirá un daño moral indemnizable –cuestión distinta será la determinación de su cuantía-¹⁹. El TJUE ha afirmado, sin embargo, que:

El incumplimiento de las normas del RGPD que atribuyen derechos al interesado (v gr. derecho de oposición) no determina por sí misma un daño inmaterial. Así se desprende de la S. 11 abril 2024, *Juris*, C-741/21)

La pérdida de control de los datos, *puede* ocasionar un daño moral: i) aunque no se haya producido un uso indebido de los mismos, o ii) aunque dure solo un breve periodo de tiempo. No obstante, será necesario demostrar que tal daño moral existe (S. 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21; S. 14 diciembre 2023, *Gemeinde Ummendorf*, C-456/22)

28. Por consiguiente, ni la vulneración de los derechos atribuidos por el RGPD al interesado, ni la pérdida de control de sus datos permiten, por sí solas, considerar existente un daño inmaterial. La cuestión es ¿cómo probar que efectivamente tal daño se ha producido?

29. El único criterio medianamente claro que cabe inferir de las sentencias analizadas es que el temor al uso indebido de los datos personales solo puede constituir daño moral si se trata de un temor *fundado*, de modo que el riesgo meramente hipotético de mal uso por parte de un tercero no da derecho a indemnización (S. 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21; S. 25 enero 2024, *MediaMarktSaturn*, C-687/21). Pero, fuera del supuesto en que existe un temor fundado a que se produzca un mal uso de los datos personales del interesado por parte de un tercero ¿qué tipo de consecuencias negativas debe acreditar éste para que efectivamente se entienda que ha sufrido un daño extrapatrimonial? La única opción plausible es tomar en consideración el sufrimiento psíquico (zozobra, agonía, ansiedad, estrés, etc.) que la infracción de que se trate haya podido causar al interesado.

hipótesis enjuiciada no hubo revelación de datos íntimos, siendo públicos los datos en cuestión, que figuraban en registros de distinta naturaleza al haberse producido diversos embargos. Es de notar que, en apoyo de su argumentación, cita las SSTJUE 4 mayo 2023, C-300/21 y 14 diciembre 2023, C-456/22, para concluir que en el caso enjuiciado no consta que la mera consulta por la demandada de los datos personales de los demandantes “tuviera ninguna trascendencia externa o su resultado fuera conocido por terceros, *ni que se causara perjuicio alguno a los demandantes*”.

¹⁸ Vid. DEL OLMO, ob. cit., pp. 202-204; GÓMEZ LIGÜERRE, ob. cit., pp. 29 y ss.

En otros países, como por ej. Alemania, cuyos tribunales han presentado varias de las cuestiones prejudiciales que han dado lugar a las sentencias comentadas, el daño moral solo se indemniza en los casos previstos en la ley (§ 253,1 BGB), lo que implica, que, al margen de normas específicas como la del RGPD, se indemniza únicamente en caso de daño corporal, a la libertad o a la autodeterminación sexual (§ 253,2 BGB). No obstante, la jurisprudencia ha reconocido también la indemnizabilidad del daño moral derivado de lesiones al denominado “derecho general de la personalidad”. En este último caso los tribunales solo reconocen indemnización en caso de vulneraciones graves de tal derecho y atribuyen a la indemnización una función preventiva además de compensatoria SPINDLER/RIECKERS, *Tort Law in Germany*, 3ª ed, Kluwer Law International, 2019, ap. 209, 239; MAGNUS, “Damages for Non-Pecuniary Loss in German Contract and Tort Law”, *The Chinese Journal of Comparative Law*, 2015 pp. 301,305, 306. Asimismo, “Damages under German Law”, en *Unification of Tort Law: Damages*, Kluwer Law International, 2001, pp. 94, 96.

Otro ejemplo es el de Austria, que ha admitido tradicionalmente la indemnizabilidad del daño moral solo cuando el causante del mismo actuó con dolo o negligencia grave (§ 1324 ABGB), aunque con alguna excepción, como cuando se ha producido una lesión corporal (§ 1325 ABGB) o en casos de lesión al derecho al honor si la difamación ha tenido lugar a través de medios de prensa. Vid. KOZIOL, “Damages under Austrian Law”, en *Unification of Tort Law: Damages*, Kluwer Law International, 2001, p. 12.

¹⁹ En este sentido SANTOS MORÓN, “La responsabilidad...” cit., pp. 249, 259.

30. Ahora bien, el TJUE ha afirmado también repetidamente, reiterando lo señalado en la S. 4 abril 2023, *Österreichische Post*, C-300/21, que no cabe establecer al efecto un umbral mínimo de gravedad. Sin embargo, no veo cómo puede llegarse a la conclusión de que las consecuencias negativas sufridas por un sujeto a consecuencia del incumplimiento de la normativa de protección de datos constituyen un daño moral si no se tiene en cuenta su entidad. Es evidente que no toda molestia o todo sentimiento de desagrado puede considerarse daño resarcible. Y la conversión de la mera incomodidad en un daño no patrimonial me parece que pasa, necesariamente, por su gravedad o intensidad. Así, por ej., nadie duda de que el ruido da lugar a un daño moral indemnizable solo cuando la molestia que provoca supera cierta intensidad o duración²⁰.

31. Por ello, me parece más atinada la postura mantenida por el Abogado General CAMPOS SÁNCHEZ-BORDONA, en las Conclusiones del Asunto *Österreichische Post*, C-300/21, en las que afirma que debe distinguirse entre daños inmateriales indemnizables y “otros inconvenientes” que por su escasa entidad, no dan derecho a compensación, correspondiendo a los jueces de los Estados miembros, llevar a cabo, en cada caso concreto, esa diferenciación²¹. En el mismo sentido se pronunció el Abogado General PITRUZZELLA, en las Conclusiones del Asunto C-340/21²².

32. En mi opinión, dado que la única forma posible de diferenciar la mera molestia, desagrado o incomodidad del daño moral es atender a la naturaleza y gravedad de la afección emocional sufrida²³, la doctrina del TJUE probablemente debe interpretarse en el sentido de que, si bien no cabe fijar “a priori” un nivel mínimo de gravedad para entender que se está ante un perjuicio indemnizable, ello no impide que el juez nacional, atendiendo a las circunstancias concretas, pueda entender que las consecuencias negativas aducidas por el perjudicado son de tan escasa entidad que no puede considerarse probado que se ha producido un daño moral. De hecho, la última resolución comentada (S. 11 abril 2024, 741/21, *Iuris*, C-741/21) parece apuntar, aunque no del todo claramente, en este sentido.

33. En cualquier caso, una vez que se estima que se está, efectivamente, ante un daño moral, la cuantificación de la indemnización, según el TJUE, deberá llevarse a cabo conforme a los criterios establecidos en cada Estado miembro (S. 4 mayo 2023, *Österreichische Post*, C-300/21)²⁴. El TJUE ha afirmado también que la gravedad de la infracción (S. 25 enero 2024, *MediaMarktSaturn*, c-687/21) o la gravedad de la culpa (S. 21 diciembre 2023, *Krankenversicherung Nordrhein*, asunto C-667/21²⁵) no pueden tenerse en cuenta a efectos de indemnización. Aunque esta postura es lógica si se parte de la función puramente indemnizatoria del art. 82 RGPD (recordemos que el TJUE niega que tenga función punitiva) conviene advertir que, cuando se trata de daños morales puros, la conducta intencional o gravemente culposa del causante del daño puede incidir en la propia entidad de este último, pues, desde el punto de vista de la afección moral, no es lo mismo ser víctima de un accidente que de un acto

²⁰ En España, en concreto, se tiene en cuenta si el ruido supera o no los niveles acústicos determinados por la normativa reglamentaria aplicable. MARTÍN VIDA, “Responsabilidad extracontractual por ruidos en Derecho alemán y en Derecho español”, *InDret*, 4/2005, p. 8.

²¹ Vid. ap. 105 y ss. En particular ap. 110 y 116.

²² El Abogado General, tras afirmar que “una interpretación amplia del concepto de daño (moral) no puede llevar a considerar que el legislador haya renunciado a la necesidad de que exista un auténtico daño” observa que debe distinguirse entre daños inmateriales indemnizables y otros inconvenientes derivados de la falta de respeto a la legalidad, como el mero sentimiento de desagrado ante tal hecho. Concluye afirmando también que corresponde a los jueces nacionales determinar cuándo se está ante meras contrariedades no indemnizables y verdaderos daños inmateriales (Vid. ap. 74 y ss.)

²³ Naturaleza y gravedad, que lógicamente, también deberán tenerse en cuenta para calcular, en su caso, la posible indemnización, de entenderse que se está, efectivamente, ante un daño moral.

²⁴ Por ej. en relación con el Derecho español se observa que, en el supuesto de acceso indebido de terceros a los datos personales, cabría tener en cuenta el tipo de dato personal afectado, el tiempo durante el cual el dato estuvo accesible y el número más o menos amplio de potenciales terceros que puedan usarlos indebidamente. MARTÍN FABÁ, ob. cit., p. 141

²⁵ Vid. infra, ap. III, B).

doloso²⁶. Por tanto, habrá que concluir que el carácter doloso o gravemente negligente podrá ser tenido en cuenta para la cuantificación de la indemnización en la medida que aumenten el perjuicio sufrido por el perjudicado.

III. Sobre el criterio de imputación de la responsabilidad y los requisitos para que exista una infracción que dé lugar a responsabilidad

34. El segundo grupo de cuestiones planteadas ante el TJUE se refiere a los requisitos para que pueda entenderse producida una infracción de la normativa de protección de datos²⁷ – concretamente una violación del principio de confidencialidad y de la seguridad de los datos personales- y al criterio de imputación de la responsabilidad derivada del art. 82 RGPD. Aunque se trata de problemas distintos, están interrelacionados, y, de hecho, en algunas de las resoluciones analizadas, además de examinarse los requisitos para que se produzca la infracción, se pronuncia el TJUE sobre el criterio de imputación de la responsabilidad.

A) No toda vulneración de la seguridad de los datos constituye una infracción

35. Comencemos por la STJUE 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21. En esta resolución, que, como antes se indicó, tiene como origen un ciberataque al sistema informático de un organismo administrativo búlgaro a raíz del cual se publicaron en internet datos personales almacenados en dicho sistema, se analiza si el ciberataque de un tercero determina necesariamente una infracción del art. 32 RGPD, relativo al deber de garantizar la seguridad de los datos personales, en relación con el 24 RGPD, que sienta el denominado principio de “responsabilidad proactiva”.

36. Conviene advertir que el art 32 RGPD obliga al responsable (y al encargado, en su caso) del tratamiento a adoptar “medidas técnicas y organizativas *apropiadas* para garantizar un *nivel de seguridad adecuado al riesgo*”²⁸. Es decir, dicho precepto no obliga al responsable del tratamiento a impedir toda violación de la seguridad y confidencialidad de los datos sino solo a adoptar medidas “apropiadas” para evitarlo, teniendo en cuenta los riesgos existentes -lo mismo se desprende, por otra parte, del art. 5,1,f)²⁹-. Por lo que respecta al art. 24 RGPD³⁰, dicho precepto dispone, con carácter general, que el responsable del tratamiento ha de aplicar medidas técnicas y organizativas *apropiadas*, tomando en consideración los riesgos existentes, para garantizar que el tratamiento es conforme con el RGPD, debiendo ser, también, capaz de demostrarlo³¹.

²⁶ MARTÍN CASALS, “La modernización del Derecho de la responsabilidad extracontractual”, en *Cuestiones actuales en materia de responsabilidad civil*, APDC, U. Murcia, 2011, p. 110; DEL OLMO, ob. cit., pp. 204, 205; 213.

²⁷ Recordemos que la existencia de una infracción es presupuesto necesario para que pueda desencadenarse la responsabilidad, junto con la existencia de daño y de relación causal entre ambos.

²⁸ El art. 32,1 dice lo siguiente: “Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán *medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo*...”

²⁹ El art. 5 RGPD, que consagra los denominados “principios del tratamiento”, dispone su apartado 1,f, respecto del principio de “integridad y confidencialidad”, estrechamente relacionado con la seguridad de los datos personales, que los datos deben ser tratados de manera “que se garantice una *seguridad adecuada* de los datos personales... mediante la aplicación de medidas técnicas u organizativas *apropiadas*”.

³⁰ Art. 24,1: “Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, *así como los riesgos* de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará *medidas técnicas y organizativas apropiadas* a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario”.

³¹ Dicho precepto -que está relacionado con el art. 25 RGPD, que consagra el denominado principio de “protección desde el diseño y por defecto”-, partiendo de una perspectiva preventiva, pretende que el responsable del tratamiento adopte ya desde el momento inicial, esto es, desde el momento de implantación del sistema a través del cual se van a tratar los datos personales,

37. Por ello, en el asunto mencionada el órgano remitente cuestiona, por lo que aquí interesa: a) si el acceso no autorizado de terceros permite por sí solo considerar que las medidas adoptadas no eran adecuadas y b) si incumbe al responsable el tratamiento la carga de probar el carácter apropiado de las mismas (cuestiones prejudiciales nº 1 y 3)³².

Una interrogante similar se plantea en el asunto *MediaMarktSaturn*, C-687/21, resuelto por la STJUE 25 enero 2024. En este caso, un empleado del responsable del tratamiento entregó por error un documento con datos personales de un cliente a otro cliente distinto, de modo que el tribunal que enjuiciaba el asunto preguntó al tribunal europeo si la entrega accidental de un documento con datos personales a un tercero supone una infracción del RGPD, y en concreto, de la obligación del responsable del tratamiento de adoptar medidas adecuadas para garantizar la seguridad de los datos (cuestión prejudicial nº 3)³³.

38. Pues bien, en la sentencia primeramente citada (S. 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21) el tribunal europeo observa que los arts. 24 y 32 RGPD se limitan a obligar 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 personales³⁴. El carácter apropiado o no de las medidas implementadas debe ser evaluado por los órganos jurisdiccionales nacionales en cada caso concreto, teniendo en cuenta los riesgos existentes y valorando si las medidas concretas implementadas se adaptan a esos riesgos³⁵ (ap. 31, 47). Dado que el art. 24 RGPD dispone que el responsable del tratamiento debe poder demostrar que las medidas adoptadas son adecuadas³⁶, no cabe entender –como si de una presunción *iuris et de iure* se tratara– que el acceso no autorizado a los datos por parte de terceros basta por sí solo para concluir lo contrario (vid. ap. 32, 34, 39). Ahora bien, la carga de la prueba del carácter apropiado de las medidas en cuestión recae sobre el responsable del tratamiento (ap. 49 y ss., ap. 57)³⁷.

39. Estas apreciaciones son reiteradas en la segunda resolución señalada (STJUE 25 enero 2024, *MediaMarktSaturn*, C-687/21) que niega que la entrega accidental de un documento con datos perso-

medidas dirigidas a garantizar que se respeta la normativa aplicable. Además, debe establecer protocolos que le permitan demostrar y acreditar la eficacia de tales medidas. Es decir, se exige del responsable del tratamiento una actitud proactiva centrada en la gestión de los riesgos potenciales asociados al tratamiento de datos. Sobre ello, vid SANTOS MORÓN, “Tratamiento de datos, sujetos implicados, responsabilidad proactiva”, cit., pp. 48 y ss.; GARCÍA HERRERA, “La responsabilidad activa en materia de protección de datos o *accountability*. Medidas de materialización”, en *Cuestiones clásicas y actuales el Derecho de daños. Estudios en Homenaje al prof. Dr. Roca Guillamón*, t. III, Thomson-Aranzadi, Navarra, 2021, pp. 795, 796; MARTÍNEZ MARTÍNEZ, R. “El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto”, en AAVV, *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales*. Valencia, Tirant Lo Blanch, 2109. pp. 316, 317.

³² El órgano remitente planteó otras dos cuestiones relacionadas con las señaladas en el texto, en concreto, qué alcance debe tener el control del juez al examinar el carácter apropiado de las medidas implantadas y si puede considerarse un informe pericial ordenado por el juez como un medio de prueba necesario y suficiente para valorar el carácter apropiado de las medidas en cuestión (vid. cuestiones prejudiciales 2 y 4).

³³ El órgano remitente preguntó además (cuestión nº 4) si la entrega accidental de un documento con datos de un tercero supone un tratamiento ilícito ex art. 5 y 24 RGPD, si bien el TJUE respondió conjuntamente a las cuestiones 3 y 4.

³⁴ El TJUE señala en ese sentido que el RGPD instaura un régimen de gestión de riesgos, pero “en modo alguno pretende eliminar los riesgos de violación de la seguridad de los datos personales” (ap. 29) y añade que “el legislador de la Unión manifestó su intención de mitigar los riesgos de violación de la seguridad de los datos personales sin pretender llegar a eliminarlos” (ap. 38).

³⁵ En relación con lo dicho el TJUE observa además que, para determinar el carácter apropiado de las medidas adoptadas, han de tenerse en cuenta, según el art. 24 RGPD, además de los riesgos, la naturaleza, el ámbito, el contexto y los fines del tratamiento. Por su parte el art. 32, que exige que las medidas sean las apropiadas para garantizar un nivel de seguridad adecuado a los riesgos, dispone que deben tenerse en cuenta también el estado de la técnica, los costes de aplicación y, nuevamente, la naturaleza, el alcance el contexto y los fines del tratamiento de que se trate. Vid. ap. 24-27.

³⁶ Recordemos que, según este precepto, el responsable del tratamiento debe, no solo garantizar que el tratamiento es conforme con el RGPD, sino que debe también “poder demostrarlo”.

³⁷ A lo dicho añade, respondiendo a la cuarta cuestión prejudicial planteada, que, para apreciar el carácter apropiado de las medidas de seguridad adoptadas por el responsable del tratamiento, “un informe pericial ordenado por el juez no constituye sistemáticamente un medio de prueba necesario y suficiente” ya que el derecho a la tutela judicial efectiva exige que el órgano jurisdiccional proceda a una apreciación objetiva del carácter apropiado de las medidas de que se trate. PLAZA PENADES, ob. cit., p. 418 indica que con ello el TJUE quiere remarcar que son admisibles todos los medios de prueba admitidos en Derecho que no pueden quedar reducidos a meras pruebas periciales.

nales de una persona a un tercero sea suficiente para considerar que las medidas adoptadas por el responsable del tratamiento no son adecuadas, en el sentido de los arts. 24 y 32 RGPD, e insiste en que el carácter apropiado de las medidas implementadas por el responsable del tratamiento debe ser valorado en el caso concreto, correspondiendo a este último la carga de probar que las medidas de seguridad en cuestión revisten tal carácter (ap. 35-45).

40. De lo expuesto se desprende que, para considerar vulnerado el art. 32 RGPD –y, en relación con éste, el art. 24–, de forma que pueda reclamarse responsabilidad (siempre que exista además daño y relación causal), es necesario que el juez concluya, tras examinar las circunstancias que rodean el caso concreto, que las medidas técnicas adoptadas por el responsable del tratamiento para garantizar la seguridad de los datos personales *no son adecuadas* al riesgo preexistente³⁸. La carga de la prueba sobre el carácter apropiado de dichas medidas pesa sobre el responsable del tratamiento.

B) ¿Responsabilidad objetiva o por culpa? Causas de exoneración de responsabilidad

41. En el mencionado asunto *Natsionalna agentsia za prihodite*, C-340/21 (STJUE 14 diciembre 2023) el órgano remitente, además de preguntar si el ciberataque llevado a cabo por terceros suponía una infracción de los arts. 24 y 32 RGPD, indaga sobre si este hecho, al ser cometido por terceros, permite excluir la responsabilidad del responsable del tratamiento (cuestión prejudicial nº 4). Esto nos lleva al siguiente aspecto a analizar, esto es, el criterio de imputación de la responsabilidad, estrechamente relacionado con las causas de exoneración admisibles.

42. No obstante, al respecto procede examinar, en primer lugar, la STJUE 21 diciembre 2023, *Krankenversicherung Nordrhein*, asunto C-667/21, que se pronuncia, específicamente, sobre si es necesaria la existencia de culpa para que se incurra en responsabilidad. En realidad en este caso, relativo a un posible tratamiento ilícito de datos de salud del demandante³⁹, la cuestión prejudicial planteada por el órgano remitente (cuestión nº 5) se refería a si es relevante el grado de culpa del responsable del tratamiento para cuantificar la indemnización y si, a tal efecto, puede tenerse en cuenta la inexistencia de culpa o la existencia de culpa leve por su parte. El TJUE observa que, para resolver esta cuestión, hay que determinar, por una parte, si la existencia o la prueba de la culpa son necesarias para que el responsable o encargado del tratamiento pueda incurrir en responsabilidad y, por otra, qué relevancia puede tener el grado de culpa en la cuantificación de la indemnización (ap. 88).

³⁸ Así, por ej., observa MARTÍN FABA, ob. cit., p. 135, podría entenderse que el responsable del tratamiento ha implementado medidas apropiadas si los ciberdelincuentes han utilizado instrumentos tan sofisticados que permiten incluso burlar las medidas de seguridad que son conformes al estado de la técnica. Y es que, como observa PLAZA PENADÉS, ob. cit., pp. 417, 418, cualquier sistema puede sufrir un ciberataque aunque tenga instalada la más alta tecnología y las mayores medidas de seguridad.

³⁹ En este supuesto un organismo público alemán que tenía la función legal de emitir informes médicos sobre la posible incapacidad laboral de personas aseguradas por la Caja de seguro obligatorio, llevó a cabo, a solicitud de esta última entidad, un informe sobre uno de sus propios empleados Para ello se puso en contacto con el médico de cabecera del empleado en cuestión. Habiendo informado ésta de tal circunstancia al mencionado empleado, el interesado pidió a una compañera del servicio informático que comprobara si efectivamente se había realizado un informe sobre su situación. La compañera de trabajo accedió a dicho informe y se lo envió. A consecuencia de ello, el demandante del litigio principal, adujo que se había producido un tratamiento ilícito de sus datos de salud, por entender que el informe debía haber sido elaborado por un organismo distinto a fin de evitar que sus compañeros tuviesen acceso a sus datos de salud. En este caso, en realidad, no estaba nada clara la existencia de la infracción del RGPD y varias de las cuestiones prejudiciales (1ª a 3ª) planteadas por el órgano remitente se refieren a la interpretación del art. 9,2,h RGPD –que, en relación con los datos de categorías especiales como son los datos de salud, permite su tratamiento con fines de medicina preventiva o laboral y evaluación de la capacidad laboral del trabajador– y del art. 6 RGPD. Aunque estas cuestiones exceden del problema aquí objeto de análisis, cabe indicar que, según el TJUE, el art. 9,2,h RGPD no impide a un organismo tratar datos relativos a la salud de sus propios empleados como “servicio médico”, ni cabe entender que el responsable del tratamiento esté obligado a garantizar que ningún compañero de trabajo del interesado pueda acceder a los datos relativos a la salud de éste. Pero, eso sí, aunque un tratamiento de datos relativos a la salud esté basado en las excepciones previstas en el art. 9, debe cumplir, además, alguna de las condiciones de licitud enunciadas en el art. 6,1 RGPD (v. gr. consentimiento del interesado, ejecución de un contrato, cumplimiento de una obligación legal, etc.) (vid. ap. 58, 70, 79).

43. Pues bien, el TJUE, tras reiterar que el art. 82,1 supedita el derecho a indemnización a la concurrencia de tres elementos, una infracción, la existencia de daño y la relación de causalidad entre ambos (ap. 90), comienza analizando el párrafo segundo del art. 82, que dispone: “cualquier responsable (del tratamiento) que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento”. Según el TJUE, este precepto presume que el responsable del tratamiento “*ha participado en la operación de tratamiento que constituye la infracción*”. No obstante, del art. 82,3 se desprende que puede quedar exonerado de responsabilidad si demuestra “*que no es en modo alguno responsable del hecho causante del daño*”.

44. A pesar de afirmar el TJUE que el art. 82 presume que el responsable del tratamiento ha cometido una infracción, de ahí deduce que el precepto establece un régimen de *responsabilidad por culpa con inversión de la carga de la prueba* (ap. 92-94)⁴⁰. Apoya esta interpretación en los arts. 24 y 32 RGPD (a los que se ha hecho referencia con anterioridad), que se limitan a obligar al responsable del tratamiento a adoptar medidas técnicas destinadas a evitar, en la medida de lo posible, cualquier violación de los datos personales (ap. 96), y observa que un mecanismo de responsabilidad por culpa con inversión de la carga de la prueba garantiza el equilibrio entre los intereses de los responsables del tratamiento y los derechos de las personas cuyos datos personales se tratan (ap. 98). Por consiguiente, concluye afirmando que la responsabilidad del responsable del tratamiento está supeditada a la existencia de culpa, la cual se presume a menos que éste demuestre que no es responsable del hecho causante del daño. Añade a lo dicho que el grado de culpa no ha de ser tenido en cuenta al fijar la indemnización (ap. 103).

45. Conviene hacer notar que en el supuesto que dio lugar al litigio al que se refiere esta sentencia, el acceso del compañero de trabajo del demandante a los datos de salud de éste se debió a su propia intervención⁴¹. Ello puede inducir a pensar que la sentencia analizada exige la culpa del responsable del tratamiento con el fin de evitar que éste incurra en responsabilidad cuando el acceso no autorizado a los datos se debe a la propia actuación del interesado. Sin embargo, tal interpretación, como observa la doctrina⁴², no resulta en absoluto necesaria, y así se desprende de las Conclusiones del Abogado General CAMPOS SÁNCHEZ-BORDONA quien, frente al criterio adoptado finalmente por el TJUE en el asunto C-667/21- estima que la responsabilidad del art. 82 es independiente de la culpa, si bien la intervención del perjudicado debe considerarse como una causa de exoneración de responsabilidad conforme al art. 82,3 RGPD (vid. ap. 73,78, 86).

46. En cualquier caso, las afirmaciones de la expresada S. 21 diciembre 2023, *Krankenversicherung Nordrhein*, C-667/21, son reiteradas en sentencias posteriores. En primer lugar, en la anteriormente mencionada S. 25 enero 2024, *MediaMarktSaturn*, C-687/21, en la que, aunque lo cuestionado era si la gravedad de la infracción debe tenerse en cuenta a efectos de indemnización (6ª cuestión prejudicial), el TJUE responde afirmando: a) que la responsabilidad queda supeditada a la existencia de culpa por parte del responsable del tratamiento, la cual se presume, salvo que éste demuestre que no es responsable del hecho generador del daño (ap. 52), y b) que, dada la finalidad indemnizatoria del art.

⁴⁰ En España también algunos autores consideran que del art. 82,3 se deduce que dicho precepto establece un sistema de responsabilidad por culpa con inversión de la carga de la prueba. 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 Protección de Datos*, Valencia, Tirant lo Blanch, 2019, p. 384; BUSTO LAGO, “Protección de datos personales y responsabilidad civil”, *Derecho de daños 2020*, pp. 481 y ss. pp. 414, 506 y ss.

⁴¹ El interesado solicitó a una compañera de trabajo del departamento informático de la empresa en la que trabajaba, que –recuérdese– había elaborado un informe sobre su capacidad laboral, que accediera a ese documento. La compañera lo hizo pese a no estar autorizada para ello, tomó fotografías de dicho informe y las remitió al interesado. Por tal motivo cabía entender que el posible daño derivado del acceso de un compañero de trabajo a los datos de salud del afectado fue debido a su propio comportamiento. Así se indica en la nota 52 de las Conclusiones del Abogado General CAMPOS SÁNCHEZ BORBONA, presentadas el 25 mayo 2023. Vid también los apartados 101 y ss.

⁴² MARTÍN FABA, ob. cit., p. 145, 146, quien señala, además, que “la introducción de la culpa del responsable como requisito para que nazca su responsabilidad no se deduce del RGPD y, más importante, no parece ayudar sino solo generar confusión”.

82 –previamente establecida por el TJUE en la S. 21 diciembre 2023, *Krankenversicherung Nordrhein*, C-667/21 - no hay que tomar en consideración la gravedad de la infracción a la hora de fijar el importe de la compensación (ap. 54, 55).

47. En el mismo sentido se pronuncia en la S. 11 abril 2024, *Juris*, C-741/21, que, en un supuesto en que se trataron los datos personales del demandante del litigio principal con fines de mercadotecnia directa pese a su expresa oposición, afirma que “de un análisis conjunto de los ap. 2 y 3 del art. 82 se desprende que éste establece un régimen de responsabilidad por culpa en el que se presume que el responsable del tratamiento ha participado en la operación de tratamiento que constituye la infracción del Reglamento” (ap. 46).

48. En mi opinión, la interpretación realizada por el TJUE en torno al criterio de imputación de responsabilidad es discutible y debe ser objeto de matización.

49. En primer lugar, si el art. 82,2 presume, como dice el TJUE en las sentencias comentadas, que el responsable del tratamiento ha participado en el hecho constitutivo de la infracción del RGPD, lo que *está presuponiendo es que ha cometido una infracción* y no, propiamente, que ha actuado de manera culposa o negligente⁴³.

Es más, aunque el TJUE interpreta que el art. 24 RGPD invierte la carga de la prueba de la culpa, lo que se infiere en realidad de este precepto es, simplemente, que el responsable del tratamiento debe demostrar que ha cumplido con la normativa de protección de datos. Es decir, lo que hace dicho precepto es *invertir la carga de la prueba de la existencia de una infracción*, no la carga de la prueba de la culpa⁴⁴. Cuestión distinta es, como se dirá después, que para que puedan considerarse infringidos ciertos preceptos del RGPD sea necesario que el responsable del tratamiento haya actuado, a su vez, negligentemente.

50. En segundo lugar, si, como dice la sentencia comentada, es necesaria la culpa para que el responsable del tratamiento puede ser condenado a indemnizar, y la culpa se presume, habría que concluir que el responsable del tratamiento podrá exonerarse de responsabilidad demostrando que actuó con la diligencia necesaria para evitar el daño. Sin embargo, no es eso lo que afirma el TJUE. Según la mencionada sentencia el responsable del tratamiento, de acuerdo con el art. 82,3 debe demostrar “que no es responsable del hecho causante del daño”⁴⁵. Pero esta circunstancia, atañe en realidad a la relación de causalidad⁴⁶, no a la culpa o negligencia, y, de hecho, así lo ha entendido el propio tribunal europeo en otras resoluciones:

- a) Así, en la S. de 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, en la que el tribunal remitente, como ya se ha avanzado con anterioridad, cuestionaba si el acceso no autorizado por parte de terceros a los datos personales, al ser consecuencia de un ciberataque, podía exonerar al responsable del tratamiento, el TJUE interpreta el art. 82,3 en el sentido

⁴³ Adviértase que, en la S. 35 enero 2024, *MediaMarktSaturn*, C-687/21, el TJUE, tras afirmar que la culpa se presume (ap. 52), continúa diciendo que el art. 82 no requiere tomar en consideración la gravedad de la *infracción* del Reglamento, *que se presume que el responsable del tratamiento ha llevado a cabo* (ap. 54). Del mismo modo, en el párrafo de la S.11 abril 2024, *Juris*, C-741/21, transcrito en el texto, se dice que el art. 82 establece un régimen de responsabilidad por culpa *en el que se presume que el responsable del tratamiento ha participado en la operación de tratamiento que constituye la infracción* del Reglamento.

⁴⁴ En este sentido SANTOS MORÓN, “La responsabilidad...”, cit., pp. 236 y ss.

⁴⁵ La versión española del art. 82,3 resulta confusa, pues en lugar de indicar que el responsable o el encargado del tratamiento quedarán exentos de responsabilidad si demuestran que no son “responsables” del hecho causante del daño, debería decir, como se deduce de las versiones francesa e italiana del precepto, que quedarán exentos de responsabilidad si demuestran que tal hecho “no les es imputable” –sobre ello SANTOS MORÓN, “La responsabilidad...” cit., p. 237-. Este es el sentido en el que, como se expresa a continuación en el texto, ha interpretado el precepto el TJUE.

⁴⁶ En esta línea DE BARRÓN ARNICHES, “Vulneraciones automatizadas del derecho a la protección de datos personales y mecanismos de tutela”, RDC, 2024, vol. IX, nº 1, p. 183; MORENO MARTÍNEZ, “El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 92 RGPD): Su posible desarrollo por el Derecho interno y problemática de coexistencia con otros mecanismos protectores”, *Cuestiones clásicas y actuales del Derecho de daños. Estudios en Homenaje al prof. Dr. Roca Guillamón*, Thomson-Aranzadi, Navarra, 2021, p. 538; HERRÁN ORTIZ, ob. cit., p. 1452.

de que el responsable del tratamiento solo puede quedar exonerado de *responsabilidad si demuestra que no existe relación de causalidad* entre su eventual incumplimiento de la obligación de protección de datos y los daños y perjuicios producidos (ap. 72).

- b) Del mismo modo, en la S. 11 abril 2024, *Juris*, C-741/21, en la que el órgano remitente preguntaba si el hecho de que la infracción cometida fuese debida a un error de una persona que actuaba bajo la autoridad del responsable del tratamiento, permitía exonerar a este último, el TJUE afirma que “las circunstancias de la exoneración establecida en el artículo 82, apartado 3, del RGPD deben limitarse estrictamente a aquellas en las que dicho responsable pueda demostrar *que el daño no le es imputable*” (ap. 70) de modo que “el referido responsable únicamente puede quedar exento de responsabilidad *si demuestra que no existe una relación de causalidad* entre el eventual incumplimiento de la obligación de protección de datos que le incumbe en virtud de los artículos 5, 24 y 32 de ese Reglamento y los daños y perjuicios sufridos por el interesado” (ap. 72). En relación con la posibilidad de que el responsable del tratamiento se exonere aduciendo el error de un auxiliar, afirma –de manera coherente con las reglas de responsabilidad por hecho ajeno- que aquél no puede liberarse de responsabilidad alegando el incumplimiento o negligencia de quien actúa bajo su autoridad⁴⁷.

51. Por consiguiente, si el responsable del tratamiento solo puede exonerarse de responsabilidad probando que el hecho causante del daño no le es imputable, por no existir realmente nexo causal entre su comportamiento y el daño, parece que la responsabilidad de dicho sujeto, una vez constatada la infracción, sería más bien objetiva que por culpa⁴⁸.

La necesidad de distinguir entre los requisitos para que exista una infracción y los requisitos para que exista responsabilidad.

52. El problema viene dado, en mi opinión, porque el TJUE –cuyos razonamientos vienen determinados, en cierta medida, por el modo en que se plantea cada cuestión prejudicial- no distingue suficientemente entre los requisitos para que exista un incumplimiento de la normativa de protección de datos y los requisitos para que tal incumplimiento desencadene responsabilidad.

53. Y la diferencia es relevante porque, como ha puesto de relieve la doctrina, las obligaciones que pesan sobre el responsable del tratamiento de acuerdo con el RGPD, son en unos casos obligaciones de “medios” y en otros de “resultado”⁴⁹. Esto implica que, mientras que, en el primer caso, para que pueda existir una infracción de la normativa de protección de datos, es preciso que el responsable del tratamiento haya actuado negligentemente, no ocurre lo mismo cuando se trata de obligaciones de resultado.

En la primera hipótesis el responsable del tratamiento podrá exonerarse de responsabilidad demostrando que actuó con la diligencia debida, y, por tanto, realmente no incumplió la normativa de protección de datos. En tal supuesto, en realidad, la prueba de la diligencia excluye la propia existencia de la infracción.

En el segundo caso en cambio (obligaciones de resultado), una vez constatada la vulneración de la normativa de protección de datos –cuya existencia es independiente de la diligencia o no del responsable del tratamiento- parece claro que este no podrá exonerarse a menos que demuestre, como establece el art. 82,3 RGPD que el daño *no le es imputable*, es decir, que se debe a *un evento ajeno a su ámbito de*

⁴⁷ La sentencia pone de manifiesto que del art. 29 RGPD se desprende que las personas que actúan bajo la autoridad del responsable solo pueden tratar los datos de acuerdo con las instrucciones de éste y de conformidad con ellas. Además, del art. 32,4 obliga al responsable del tratamiento a adoptar medidas para garantizar que cualquier persona que actúe bajo su autoridad siga sus instrucciones. Es decir, corresponde al responsable del tratamiento asegurarse de que sus empleados apliquen correctamente sus instrucciones (vid. ap. 47-49)

⁴⁸ Así lo entendió, como se ha dicho antes, el Abogado General CAMPOS SÁNCHEZ-BORDONA, en sus Conclusiones al Asunto C-667/21, presentadas el 24-5-2023.

⁴⁹ VAN ALSENOY, “Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation”, *JPIITEC*, 2016, 271, p. 282; el mismo autor *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, 2019, p. 103, 104. RUBÍ PUIG, “Daños por infracción del derecho a la protección de datos personales, El remedio indemnizatorio del art. 82 RGPD”, *RDC*, 2018, vol. V, n° 4, p. 58.

control, como sería el comportamiento de la víctima, el hecho de un tercero imprevisible e inevitable o, en general, un supuesto de fuerza mayor⁵⁰.

54. Conviene advertir, en relación con ello, que los actos llevados a cabo por los auxiliares o empleados del responsable del tratamiento no pueden considerarse como un evento ajeno a su ámbito de control. Así se desprende de la mencionada STJUE 11 abril 2024, *Iuris*, C-741/21, que, como se ha dicho, afirma que el responsable del tratamiento no puede liberarse de responsabilidad alegando el incumplimiento o negligencia de quien actúa bajo su autoridad. El ciberataque cometido por un tercero podría, en cambio, excluir la responsabilidad del responsable (o encargado) del tratamiento, toda vez que no tenga su origen en la deficiente adopción de medidas de seguridad⁵¹.

55. De hecho, el ejemplo, quizás, más claro, de *obligación de medios* impuesta al responsable del tratamiento es la que atañe, precisamente, a la adopción de medidas de seguridad. Como se ha visto, el art. 32 RGPD solo obliga al responsable del tratamiento a adoptar las medidas técnicas y organizativas que sean “apropiadas para garantizar un nivel de seguridad adecuado al riesgo”. Por consiguiente, para determinar que efectivamente se ha incumplido dicho precepto es necesario valorar la diligencia del responsable del tratamiento a la hora de adoptar las medidas de seguridad en cuestión⁵², si bien, teniendo en cuenta lo dispuesto en el art. 24,1 RGPD –que impone al responsable del tratamiento la carga de acreditar el cumplimiento normativo- debe entenderse que corresponde a este último demostrar el carácter “apropiado” de las medidas implementadas.

56. Por el contrario, tratándose del cumplimiento de los principios del tratamiento, 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 deduce que aquél queda obligado a obtener un resultado, sin que sea suficiente con que adopte medidas *apropiadas* dirigidas a asegurarlo (art. 24)⁵³. Así ocurre, por ej., en relación con el principio de licitud, que exige que todo tratamiento de datos personales se haga con consentimiento del interesado, a menos que concurra alguna de las bases de legitimación establecidas en el art. 6 RGPD. Si, por ej., el responsable de una red social, solicita a través de su página web el consentimiento de los usuarios para tratar sus datos personales con ciertos fines, pero, sin embargo, trata erróneamente los datos de un usuario que no ha consentido (o no ha consentido para ese fin específico) ¿acaso

⁵⁰ En este sentido SANTOS MORÓN, “La responsabilidad...” cit., p. 237; VAN ALSENOY, “Liability under EU Data Protection Law...” cit., p. 283; RUBÍ PUIG, ob. cit., p. 78; MORENO MARTÍNEZ, ob. cit., p. 538; HERRÁN ORTIZ, ob. cit., p. 1452.

⁵¹ Por ello afirma la repetida STJUE 14 diciembre 2023, *Natsionalna agentsia za prihodite*, C-340/21 (ap. 71), que la violación de la seguridad de los datos personales cometidas por cibercriminales no puede imputarse al responsable del tratamiento, a menos que este último “*la hubiera hecho posible* por incumplir alguna obligación establecida en el RGPD y, en particular, la obligación de protección de datos a la que está sujeto en virtud de los arts. 5,1,f), 24 y 32 del mismo Reglamento”.

⁵² En España, la STS (Sala 3ª) 14 febrero 2022 (RJ 2022/1280), en relación con un procedimiento sancionador por infracción de la seguridad de los datos personales (regulada en el art. 9 de la anterior LOPD - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal-) ya afirmó que la obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales “*no puede considerarse una obligación de resultado*, que implique que produzca una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento”.

⁵³ Ello es así salvo que de la definición del concreto principio del tratamiento se deduzca lo contrario. Es lo que ocurre, por ej., en relación con el principio de exactitud, ya que el art. 5,1,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 REIGADA, “Los principios relativos al tratamiento (Comentario al art. 5 RGPD y al art. 4 LOPDGD)”, 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.

¹o mismo ocurre cuando se trata del principio de “integridad y confidencialidad” –relacionado, como se ha dicho, con la seguridad de los datos, art. 32 RGPD- ya que el art. 5,1,f) solo exige que los datos se traten de manera que se garantice una seguridad “*adecuada*”, mediante la aplicación de medidas técnicas y organizativas “*apropiadas*”.

cabe pensar que podrá eximirse de responsabilidad demostrando que adoptó medidas técnicas adecuadas para recabar el consentimiento de los usuarios de su página web?⁵⁴ Lo lógico es entender que en este caso el responsable del tratamiento solo podrá exonerarse demostrando que el tratamiento de datos ilícito se debe a un hecho externo, imprevisible e inevitable, ajeno a su esfera de control (art. 82,3 RGPD)⁵⁵.

57. En mi opinión puede decirse que, pese a que en las resoluciones del TJUE examinadas se afirma que la responsabilidad del responsable del tratamiento requiere que exista culpa o negligencia, ello es así, propiamente, cuando el incumplimiento de la normativa de protección de datos presupone un comportamiento negligente del responsable del tratamiento, como sucede cuando se trata del cumplimiento del deber de seguridad (art. 32 RGPD). En tal caso el demandado podrá exonerarse de responsabilidad demostrando que actuó con la diligencia debida, lo que en realidad excluye la existencia de la infracción. En los casos –menos frecuentes– en que pesa sobre dicho sujeto una obligación de resultado, la no obtención del mismo supone una vulneración de la normativa aplicable que desencadenará su responsabilidad, a menos que, conforme al art. 82,3 RGPD, el responsable del tratamiento demuestre que el hecho causante del daño no le es imputable.

Conclusiones

58. De la jurisprudencia examinada se desprende que no toda infracción de la normativa de protección de datos genera un daño. El sujeto que pretenda obtener indemnización deberá probar que dicha infracción le ha producido algún perjuicio efectivo. Este perjuicio puede ser patrimonial (“material” según la terminología empleada en el RGPD) o no patrimonial (“inmaterial”). Pero el hecho de que se vulneren los derechos que el RGPD reconoce al perjudicado (v. gr. acceso, rectificación, oposición, cancelación), o el hecho de que sus datos se traten de forma ilícita –esto es, sin su consentimiento y sin que exista otra base de legitimación–, aunque suponga una “pérdida del control” de dichos datos, tampoco genera por sí mismo un daño moral.

59. Según el TJUE el interesado debe demostrar que las “consecuencias negativas” que ha sufrido constituyen “daño inmaterial”. El problema es que es difícil dilucidar en la práctica, cuando se está ante tal tipo de daño. Un ejemplo, además de los casos en que se vulneran otros derechos de la personalidad del individuo como su honor o intimidad, es el supuesto en que, aun no habiéndose producido un mal uso de los datos personales del afectado, existe un temor, fundado en circunstancias objetivas, a que ello tenga lugar en el futuro. Pero, fuera de esa hipótesis el perjudicado deberá demostrar que ha sufrido un perjuicio emocional digno de ser considerado como “daño inmaterial”. Ahora bien, para concluir que así es debe tenerse en cuenta necesariamente la entidad, gravedad o intensidad de dicho perjuicio. Aunque el TJUE ha afirmado en la mayoría de las sentencias analizadas que no cabe establecer un umbral mínimo de gravedad para que el daño resulte indemnizable, no se ve cómo puede diferenciarse la mera molestia o contrariedad del verdadero daño moral si no se atiende a su gravedad. Así parece admitirlo, aunque tímidamente, la última de las sentencias emitidas por el TJUE en esta materia, la S. 11 abril 2024, *Iuris*, C-741/21. Queda por ver, no obstante, cómo evolucionará la doctrina del TJUE en el futuro⁵⁶.

⁵⁴ Adviértase que el art. 7,1 RGPD dispone que “cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que *aquel consintió el tratamiento de sus datos personales*”. No basta, por consiguiente, con adoptar medidas “apropiadas” para obtener tal consentimiento, sino que es preciso que el consentimiento concurra de modo efectivo.

⁵⁵ Cabe, no obstante, apreciar cierta excepción 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, el art. 8,2 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”.

⁵⁶ Vid. SANTOS MORÓN, “La responsabilidad...” cit., pp. 239 y ss.

⁵⁶ En el momento de escribir estas líneas está pendiente todavía la resolución del asunto C-590/22, que plantea cuestiones prejudiciales similares a las aquí analizadas.

60. Dado que el TJUE considera, con buen criterio, que el art. 82 RGPD tiene función indemnizatoria, niega que la gravedad de la infracción o la gravedad de la culpa deban ser tenidas en cuenta para calcular la indemnización. Sin embargo, hay que tener presente que el carácter doloso o gravemente negligente de la conducta del demandado puede incrementar el perjuicio emocional sufrido por el afectado, por lo que en tal caso podrá influir en el importe de la indemnización.

61. La jurisprudencia examinada, por otra parte, pone de manifiesto que para considerar incumplido el deber de “seguridad del tratamiento” regulado en el art. 32 RGPD -estrechamente ligado al principio de “integridad y confidencialidad” de los datos personales del art. 5,1,f)-, no basta con que se haya producido un acceso indebido a los datos por parte de terceros (sean consecuencia de un ciberataque, de un error material padecido por un empleado del responsable del tratamiento o de otro hecho) sino que es preciso concluir, atendiendo a las circunstancias del caso concreto, que las medidas de seguridad adoptadas por el responsable del tratamiento no eran las “apropiadas” para el riesgo preexistente, lo que obliga a valorar la diligencia empleada por tal sujeto en la adopción de tales medidas. La carga de la prueba de que las medidas adoptadas eran apropiadas corresponde al responsable del tratamiento de acuerdo con el art. 24 RGPD.

62. En el supuesto enunciado, para que exista una vulneración del art. 32 RGPD es necesario que el responsable del tratamiento haya actuado culposa o negligentemente. Es decir, la culpa es presupuesto de la existencia de la propia infracción. De ahí que, como ha afirmado el TJUE, no pueda desencadenarse la responsabilidad del responsable del tratamiento sin que medie culpa por su parte. En la medida en que la carga de la prueba de que se adoptaron las medidas adecuadas para evitar la infracción corresponde al responsable del tratamiento, es lógico concluir también que la “culpa” se presume.

63. Ahora bien, no en todos los casos puede aplicarse este planteamiento. Aunque el TJUE ha mantenido que la responsabilidad exigible ex art. 82 RGPD se basa en la culpa, si bien esta se presume, en los supuestos en que el responsable del tratamiento está obligado a obtener un resultado (v. gr. contar con el consentimiento del interesado si no hay otra base que legitime el tratamiento de sus datos), la existencia de la infracción es independiente de su culpa o negligencia⁵⁷ Por ello no parece que en tal hipótesis el demandado pueda exonerarse de responsabilidad aduciendo que actuó diligentemente y adoptó *medidas apropiadas* para evitar el incumplimiento normativo y, por ende, el posible daño. En tal caso, el responsable del tratamiento solo podrá exonerarse, de acuerdo en el art. 82,3 RGPD, demostrando que la infracción ha sido provocada por un evento *ajeno a su ámbito de control*, de modo que su comportamiento no puede ser considerado como causa del daño.

⁵⁷ Es decir, no depende de que el responsable del tratamiento haya adoptado o no medidas “apropiadas” para obtener el resultado deseado. Basta con la no consecución del mismo para que exista una infracción.