Revista CESCO de Derecho de Consumo
http://revista.uclm.es/index.php/cesco

Nº 49/2024
ISSN 2254-2582

https://doi.org/10.18239/RCDC_2024.49.3474

NOVEDADES EN MATERIA DE INDEMNIZACIÓN Y PROTECCIÓN DE DATOS PERSONALES*

José María Martín Faba
Profesor Ayudante Doctor UAM
Centro de Estudios de Consumo

Resumen: Son aún escasas las sentencias del Tribunal de Justicia de la Unión Europea que proporcionan interpretaciones de preceptos del Reglamento de Protección de Datos que regulan la responsabilidad y el derecho a indemnización. En consecuencia, el significado y el alcance de estas disposiciones genera todavía muchas incógnitas. Con todo, la situación está cambiando de forma paulatina, pues recientemente el Tribunal de Justicia ha dictado varias resoluciones que enuncian interpretaciones inéditas de preceptos del Reglamento relativos a la responsabilidad y al derecho a indemnización. En el presente artículo se exponen las interpretaciones enunciadas por el Tribunal de Justicia en dos de sus últimas sentencias y se realizan una serie de valoraciones sobre cada una de ellas.

Palabras clave: Datos personales, responsabilidad civil, indemnización.

Title: News on liability and protection of personal data.

Abstract: There are still few rulings from the Court of Justice of the European Union that provide interpretations of the provisions of the Data Protection Regulation that regulate liability and the right to compensation. Consequently, the meaning and scope of these provisions is currently poorly defined. However, the situation is changing, as the Court of Justice has recently issued several resolutions that set out unprecedented interpretations of the provisions of the Data Protection Regulation relating to liability.

* Trabajo realizado en el marco del Proyecto de Investigación PID2021-128913NB-I00, del Ministerio de Ciencia e Innovación y la Agencia Estatal de Investigación (AEI) cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER) titulado "Protección de consumidores y riesgo de exclusión social: seguimiento y avances", dirigido por Ángel Carrasco Perera y Encarna Cordero Lobato; en el marco de las Ayudas para la realización de proyectos de investigación aplicada, en el marco del Plan Propio de investigación, cofinanciadas en un 85% por el Fondo Europeo de Desarrollo Regional (FEDER), para el proyecto titulado "Modelos jurídicos eficientes de consumo sostenible", con Ref.: 2022-GRIN-34487 dirigido por Ángel Carrasco Perera y Ana I. Mendoza Losana y en el marco del Proyecto de Investigación SBPLY/23/180225/000242 "El reto de la sostenibilidad en la cadena de suministros y la defensa del consumidor final" cofinanciadas por el Fondo Europeo de Desarrollo Regional, en el marco del Programa Operativo de Castilla-La Mancha 2021-2027 dirigido por Ángel Carrasco Perera y Ana Carretero Garcia.

This article sets out the interpretations set forth by the Court of Justice in its last two rulings and makes comments on each of them.

Key words: Personal data, liability, compensation.

1. INTRODUCCIÓN

Hasta hace un tiempo relativamente reciente, no existían sentencias del Tribunal de Justicia de la Unión Europea (en adelante, TJUE) que interpretaran y desarrollaran las disposiciones que regulan la responsabilidad civil y el derecho a indemnización en el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD). En consecuencia, el significado y alcance de estas disposiciones genera todavía muchas incógnitas.

Rompió esta tendencia la sentencia de 4 de mayo de 2023, asunto C-300/21, *UI* y *Österreichische Post AG* (EU:C:2023:3709), en la que el TJUE, interpretando el artículo 82 RGPD, ha establecido que la mera infracción de las disposiciones del RGPD no basta para reconocer un derecho a indemnización, que no puede supeditarse la indemnización por daños inmateriales a que los daños hayan alcanzado cierto grado de gravedad y que para determinar el importe de la indemnización los jueces nacionales deben aplicar las normas internas de cada Estado miembro, siempre que respeten los principios de equivalencia y de efectividad.

Posteriormente, el TJUE ha dictado dos sentencias que incorporan las doctrinas anteriores y proporcionan, además, interpretaciones inéditas sobre disposiciones relativas a la responsabilidad civil y el derecho a indemnización en el ámbito del RGPD. Por un lado, la sentencia de 14 de diciembre de 2023, asunto C-340/21, *VB y Natsionalna agentsia za prihodite* (ECLI:EU:C:2023:986) y, por otro, la sentencia de 21 de diciembre de 2023, asunto C-667/21, *ZQ y Medizinischeres* (ECLI:EU:C:2023:1022).

A continuación, expondremos los hechos de los dos últimos asuntos referenciados, la fundamentación y respuestas del TJUE a las preguntas planteadas por los tribunales remitentes y unos comentarios sucintos relacionados con cada una de las doctrinas emitidas.

2. ASUNTO C-340/21

2.1. Hechos

La *Natsionalna agentsia za prihodite* (en adelante, NAP) es una autoridad dependiente del Ministro de Hacienda búlgaro. En el marco de sus funciones, que consisten, entre otras, en la identificación, el aseguramiento y el cobro de los créditos de carácter público, es responsable del tratamiento de datos personales, con arreglo al artículo 4.7 RGPD.

Con ocasión de un ciberataque, se produjo un acceso no autorizado al sistema informático de la NAP, publicándose en Internet datos personales almacenados en dicho sistema. Más de seis millones de personas físicas se vieron afectadas por estos hechos. Cientos de ellas ejercieron acciones contra la NAP, reclamando una indemnización por los daños y perjuicios inmateriales supuestamente derivados de la comunicación de sus datos personales.

Uno de los afectados interpuso ante el Tribunal de lo Contencioso-Administrativo de Sofía una demanda mediante la que solicitaba que la NAP le abonara la cantidad de 1.000 levas búlgaras (510 euros) en concepto de indemnización por daños y perjuicios, en virtud del artículo 82 RGPD. La demandante alegó que había sufrido un perjuicio inmaterial derivado de la violación de la seguridad de los datos personales derivada del incumplimiento por parte de la NAP de las obligaciones que le incumbían en virtud de los artículos 5.1 f), 24 y 32 RGPD. La demandante alega un daño inmaterial consistente en el temor a que sus datos personales, publicados sin su consentimiento, sean objeto de un uso indebido en el futuro, o a que ella misma sea víctima de un chantaje, una agresión o incluso un secuestro.

En su defensa, la NAP alegó que había adoptado todas las medidas necesarias, con anterioridad, para evitar la violación de la seguridad de los datos personales almacenados en su sistema informático y, posteriormente, para limitar los efectos de dicha violación y tranquilizar a los ciudadanos. Además, sostuvo que no existía relación de causalidad entre el perjuicio inmaterial alegado y la citada violación. Por último, adujo que, al haber sido objeto, ella misma, de un ataque doloso por parte de personas que no eran empleados suyos, no podía ser considerada responsable de las consecuencias perjudiciales del mencionado ataque.

Pues bien, el Tribunal de lo Contencioso-Administrativo de Sofía desestimó la demanda. Consideró, por un lado, que el acceso no autorizado a la base de datos de

la NAP se debió a un ciberataque cometido por terceros y, por otro lado, que la demandante no había demostrado que la NAP no hubiera adoptado medidas de seguridad. Además, estimó que la demandante no había sufrido daño o perjuicio inmaterial alguno que diera derecho a indemnización.

La demandante interpuso un recurso de casación contra la mencionada resolución ante el Tribunal Supremo de lo Contencioso-Administrativo de Bulgaria, que es el órgano jurisdiccional remitente. En su recurso de casación, la demandante sostiene que el tribunal de primera instancia incurrió en error de Derecho a la hora de distribuir la carga de la prueba relativa a las medidas de seguridad adoptadas por la NAP y que esta última no había demostrado que no había incumplido sus obligaciones a este respecto. La demandante también alega que el temor a que sus datos personales puedan utilizarse indebidamente en el futuro constituye un perjuicio inmaterial real y no hipotético.

En estas circunstancias, el Tribunal Supremo de lo Contencioso-Administrativo de Bulgaria decidió suspender el procedimiento y plantear al TJUE una serie de cuestiones prejudiciales.

2.2. Doctrina del TJUE

2.2.1. Un ciberataque no basta para concluir que las medidas de seguridad adoptadas no son apropiadas

El tribunal remitente pregunta si los artículos 24 y 32 RGPD deben interpretarse en el sentido de que una comunicación no autorizada de datos personales o un acceso no autorizado a tales datos por parte de terceros bastan, por sí solos, para considerar que las medidas técnicas y organizativas adoptadas por el responsable del tratamiento no eran "apropiadas" con arreglo a los citados artículos 24 y 32.

Según el TJUE, los artículos 24 y 32 RGPD no pueden entenderse en el sentido de que un acceso no autorizado de datos personales por parte de terceros basta para concluir que las medidas adoptadas por el responsable del tratamiento no eran apropiadas, sin siquiera permitir a este último aportar la prueba en contrario. Por un lado, el artículo 24 RGPD establece que el responsable del tratamiento debe poder demostrar la conformidad con el RGPD de las medidas que ha adoptado, posibilidad de la que se vería privado si se admitiera una presunción *iuris et de iure.* De otro, tanto el artículo 24.3 como el artículo 32.3 RGPD indican que el responsable o el encargado del tratamiento pueden demostrar que han cumplido los requisitos de los artículos 24.1 y 32.1 RGPD, basándose en que se han adherido a un código de conducta aprobado o a un mecanismo de certificación aprobado. Finalmente, del artículo 82.3 RGPD se desprende que, si bien un responsable del tratamiento es responsable del daño causado por un tratamiento que constituya una infracción del RGPD, queda exonerado de responsabilidad si demuestra que "no es en modo alguno responsable" del hecho que haya causado los daños.

En consecuencia, el TJUE responde a la cuestión prejudicial que los artículos 24 y 32 RGPD deben interpretarse en el sentido de que una comunicación no autorizada de datos personales o un acceso no autorizado a tales datos por parte de terceros no bastan, por sí solos, para considerar que las medidas técnicas y organizativas adoptadas por el responsable del tratamiento no eran "apropiadas" con arreglo a los citados artículos.

Comentario: Una brecha de datos personales, ocasionada por un ciberataque, no es suficiente para concluir que el responsable del tratamiento ha infringido el artículo 32 RGPD, por no implementar las medidas de seguridad apropiadas. Tampoco basta para concluir que el responsable ha incumplido el artículo 32 RGPD el que un trabajador del responsable haya entregado por error a un tercero no autorizado un documento que contenía datos personales del demandante[1].

En consecuencia, la obligación establecida en el artículo 32 RGPD no puede entenderse incumplida por el hecho de producirse un acceso o comunicación no autorizada de los datos personales. La obligación de implementar medidas de seguridad apropiadas no trataría de garantizar el resultado de la seguridad plena de los datos personales y la inexistencia de quiebras de seguridad, sino tan solo de procurar, en la medida de lo posible, la seguridad de los datos personales. Entonces, la obligación de adoptar medidas de seguridad apropiadas se entiende cumplida cuando el responsable actúa conforme al estándar de diligencia y los criterios enunciados en el artículo 32 RGPD, independientemente de que llegue a producirse una brecha de los datos personales[2].

En otras palabras, cuando se produce una violación de los datos personales, el responsable del tratamiento no responde objetivamente, sino que podrá probar que adoptó las medidas de seguridad apropiadas, actuando conforme al estándar de diligencia previsto en el artículo 32 RGPD. Así, podría entenderse que el responsable del tratamiento ha implementado las medidas de seguridad apropiadas si los ciberdelincuentes han utilizado instrumentos tan sofisticados que permiten burlar incluso las medidas de seguridad que son conformes con el "estado de la técnica"[3].

2.2.2. Evaluación de toda la estrategia empresarial sobre la seguridad de los datos

El tribunal remitente pregunta si el artículo 32 RGPD debe interpretarse en el sentido de que el carácter apropiado de las medidas técnicas y organizativas adoptadas por el responsable del tratamiento en virtud de dicho artículo debe ser apreciado por los

[1] STJUE de 25 de enero de 2024, asunto C-687/21, *BL y MediaMarktSaturm* (ECLI:EU:C:2024:72).
[2] STS 188/2022 (Sala 3.ª) de 15 febrero (ECLI:ES:TS:2022:5432).
[3] La SAN de 25 de febrero de 2010 (JUR 2010/82723) resuelve un caso en el que un sujeto con altos conocimientos técnicos vulneró las medidas de seguridad implementadas por una web, obteniendo datos de los usuarios de dicha web que publicó posteriormente en internet. La sentencia considera que el responsable del tratamiento había adoptado medidas de seguridad apropiadas, por lo que no podía responsabilizársele del acceso indebido del tercero a los ficheros.

jueces nacionales en cada caso concreto, en particular teniendo en cuenta los riesgos vinculados al tratamiento de los datos.

Según el TJUE, el responsable del tratamiento dispone de cierto margen de apreciación para determinar cuáles son las medidas técnicas y organizativas apropiadas a fin de garantizar un nivel de seguridad adecuado al riesgo, como exige el artículo 32.1 RGPD. Por tanto, para controlar el carácter apropiado de las medidas técnicas y organizativas adoptadas, el juez nacional no debe limitarse a comprobar de qué manera el responsable del tratamiento ha procurado cumplir con las obligaciones que le incumben en virtud de dicho artículo, sino que debe llevar a cabo un examen en cuanto al fondo de estas medidas, a la luz de todos los criterios a que hace referencia el mencionado artículo, así como de las circunstancias propias del caso y de los elementos de prueba de que dispone el órgano jurisdiccional nacional a estos efectos.

Así pues, el TJUE responde a la cuestión prejudicial que el artículo 32 RGPD debe interpretarse en el sentido de que el carácter apropiado de las medidas técnicas y organizativas adoptadas por el responsable del tratamiento en virtud de dicho artículo debe ser apreciado por los órganos jurisdiccionales nacionales en cada caso concreto, teniendo en cuenta los riesgos vinculados al tratamiento y apreciando si la naturaleza, el contenido y la adopción de esas medidas están adaptados a estos riesgos.

Comentario: El estándar de cumplimiento exigido por el artículo 32 RGPD ("aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo") está condicionado por multitud de criterios y sujeto a ponderación, por lo que la comprobación de si un determinado comportamiento se ajusta a él solo puede realizarse teniendo en cuenta las circunstancias del caso concreto. En consecuencia, el cumplimiento de medidas técnicas puntuales, como la pseudonimización o cifrado de los datos, u organizativas, como la adhesión a códigos de conducta o a mecanismos de certificación, no supone, por sí solo, considerar que las medidas de seguridad adoptadas son apropiadas. Así, el TJUE asume una especie de principio general según el cual el cumplimiento por parte del demandado de reglamentos y normas técnicas no es causa de exoneración de responsabilidad, debiendo tenerse en cuenta todas las circunstancias para determinar si su actuación ha sido conforme al artículo 32 RGPD.

2.2.3. El responsable del tratamiento soporta la carga de la prueba del carácter apropiado de las medidas de seguridad

El tribunal remitente pregunta si el principio de responsabilidad del responsable del tratamiento, enunciado en el artículo 5.2 RGPD y desarrollado en el artículo 24 RGPD, debe interpretarse en el sentido de que, en el marco de una acción de indemnización basada en el artículo 82 RGPD, el responsable del tratamiento soporta la carga de la prueba del carácter apropiado de las medidas de seguridad que ha adoptado con arreglo al artículo 32 RGPD.

A este respecto, el TJUE recuerda que el artículo 5 RGPD establece que el responsable del tratamiento debe ser capaz de demostrar la conformidad del tratamiento con los principios relativos al tratamiento de datos personales enunciados en dicho precepto. Asimismo, señala que tanto el artículo 24.1 RGPD como el artículo 32.1 RGPD obligan al responsable del tratamiento a aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y *poder demostrar* que el tratamiento es conforme con el RGPD. Estos tres artículos establecen una regla general que, a falta de indicación contraria en el RGPD, debe aplicarse también en el marco de una acción de indemnización basada en el artículo 82.

En consecuencia, el TJUE responde a la cuestión prejudicial que el principio de responsabilidad del responsable del tratamiento, enunciado en el artículo 5.2 RGPD y desarrollado en el artículo 24 RGPD, debe interpretarse en el sentido de que, en el marco de una acción de indemnización basada en el artículo 82 RGPD, el responsable del tratamiento soporta la carga de la prueba del carácter apropiado de las medidas de seguridad que ha adoptado con arreglo al artículo 32 RGPD.

Comentario: En una demanda basada en el artículo 82 RGPD, el interesado debe demostrar que se ha producido una infracción del RGPD, que ha sufrido un daño y que existe una relación de causalidad entre estos dos elementos. Con todo, cuando la infracción del RGPD está relacionada con la falta de implementación de las medidas de seguridad apropiadas, en el sentido del artículo 32 RGPD, la carga de la prueba no puede llegar hasta el extremo de exigir al demandante acreditar que tales medidas técnicas y organizativas aplicadas por el responsable del tratamiento no son apropiadas.

La inversión de la carga de la prueba de la adecuación de las medidas de seguridad es acertada, porque los interesados no tienen conocimientos suficientes para entenderlas, ni disponen de acceso a toda la información que posee el responsable del tratamiento en lo que respecta a la implementación de tales medidas. Es lógico que quienes posean más conocimientos sobre el tratamiento de datos y un mayor control sobre las medidas de ciberseguridad asuman, por las facilidades que tienen, la carga de demostrar la adecuación de dichas medidas al estándar del artículo 32 RGPD (art. 217.7 LEC).

2.2.4 Un informe pericial ordenado por el juez no constituye sistemáticamente un medio de prueba necesario y suficiente

El tribunal remitente pregunta si el artículo 32 RGPD y el principio de efectividad del Derecho de la Unión deben interpretarse en el sentido de que, para apreciar el carácter apropiado de las medidas de seguridad que el responsable del tratamiento ha adoptado en virtud de dicho artículo, un informe pericial ordenado por el juez constituye un medio de prueba necesario y suficiente.

Según el TJUE, corresponde a cada Estado miembro establecer las reglas relativas a los medios de prueba que permiten evaluar el carácter apropiado de las medidas,

siempre que se respeten los principios de equivalencia y efectividad. En el presente asunto, el TJUE duda de que se respete el principio de efectividad, en la medida en que el propio tenor de la cuestión prejudicial presenta el peritaje judicial como un "medio de prueba necesario y suficiente".

Así, el recurso sistemático a dicho informe pericial puede resultar superfluo a la vista de las demás pruebas en poder del tribunal nacional, como los resultados de un control del cumplimiento de las medidas de protección de datos personales llevado a cabo por una autoridad independiente y establecido por la ley, siempre que dicho control sea reciente. Además, no se llevaría a cabo una apreciación objetiva de las medidas de seguridad adoptadas por el responsable si un órgano jurisdiccional nacional pudiera deducir exclusiva o automáticamente de un informe pericial que las medidas de que se trate son "apropiadas".

En suma, el TJUE responde a la cuestión prejudicial que el artículo 32 RGPD y el principio de efectividad del Derecho de la Unión deben interpretarse en el sentido de que, para apreciar el carácter apropiado de las medidas de seguridad que el responsable del tratamiento ha adoptado en virtud de dicho artículo, un informe pericial ordenado por el juez no constituye sistemáticamente un medio de prueba necesario y suficiente.

Comentario: En consonancia con la necesidad de evaluación circunstanciada de la adecuación de las medidas de seguridad, el TJUE considera que los tribunales nacionales deben considerar una amplia gama de pruebas y que la determinación de si las medidas son adecuadas no puede depender exclusivamente de un informe pericial ordenado por el juez. Con todo, debido a la complejidad que supone probar un hecho como la adecuación de las medidas de seguridad al artículo 32 RGPD, es probable que no haya disponible un gran abanico de pruebas que proporcionen fiabilidad y objetividad. El TJUE pone como ejemplo de prueba fiable y objetiva un informe pericial reciente sobre el control del cumplimiento de las medidas de seguridad, llevado a cabo por una autoridad independiente.

2.2.5 El responsable del tratamiento no queda exonerado por el mero hecho de que los daños resulten de un ciberataque

El tribunal remitente pregunta si el artículo 82.3 RGPD debe interpretarse en el sentido de que el responsable del tratamiento está exonerado de la obligación de indemnizar los daños sufridos por una persona, por el mero hecho de que esos daños resulten de una comunicación no autorizada de datos personales o de un acceso no autorizado a esos datos por parte de "terceros", a los efectos del artículo 4.10 RGPD.

El TJUE recuerda, en primer lugar, que el artículo 82.2 RGPD dispone que "cualquier responsable 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 Reglamento" y, en segundo lugar, que el artículo 82.3 RGPD establece que un

responsable o encargado del tratamiento, según los casos, quedará exento de tal responsabilidad "si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios".

Cuando la violación de la seguridad de los datos personales ha sido cometida por cibercriminales y, por tanto, por "terceros", esa violación no puede imputarse al responsable del tratamiento, salvo 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 artículos 5.1 f), 24 y 32 RGPD. Así pues, en caso de violación de la seguridad de los datos personales por parte de un tercero, el responsable del tratamiento puede quedar exonerado de responsabilidad, al amparo del artículo 82.3 RGPD, si demuestra que no existe relación de causalidad entre su eventual incumplimiento de la obligación de protección de datos y los daños y perjuicios sufridos por la persona física.

En conclusión, el TJUE responde a la cuestión prejudicial que el artículo 82.3 RGPD debe interpretarse en el sentido de que el responsable del tratamiento no puede quedar exonerado de la obligación de indemnizar los daños y perjuicios sufridos por una persona, con arreglo artículo 82.1 y 2 RGPD, por el mero hecho de que esos daños y perjuicios resulten de una comunicación no autorizada de datos personales o de un acceso no autorizado a esos datos por parte de "terceros", pues ese responsable debe demostrar que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios en cuestión.

Comentario: El responsable del tratamiento no quedará exonerado por la mera prueba de que la vulneración de los datos se produjo por un ciberataque. Nótese que cuando un responsable del tratamiento es víctima de un ataque por parte de un ciberdelincuente, puede que la falta de adopción de medidas de seguridad apropiadas haya facilitado o contribuido a la producción del daño. En efecto, el demandado no puede invocar el artículo 82.3 RGPD, alegando que "no es en modo alguno responsable del hecho que haya causado los daños y perjuicios", si el daño ha sido propiciado, precisamente, por la infracción de las normas que regulan la actuación del responsable del tratamiento en cuanto a las medidas de seguridad (art. 32 RGPD). Sería algo similar a la responsabilidad (aquí contractual) del Metro de Madrid por la paliza propinada por un tercero a un pasajero, cuando se demuestra que la agresión se ha producido por el incumplimiento de la obligación de prestar el servicio con diligencia y cuidado, en condiciones óptimas de seguridad[4].

Si el responsable acredita que implementó medidas de seguridad apropiadas y que aun así se produjo un acceso no autorizado a los datos, entonces no nacerá el derecho a indemnización del artículo 82.1 RGPD, porque el responsable no ha infringido el RGPD, no siendo necesario acudir al artículo 82.3 RGPD. Este precepto faculta al responsable a exonerarse si prueba que "no es en modo alguno responsable del hecho

[4] STS 6277/2008 (ECLI:ES:TS:2008:6277).

que haya causado los daños y perjuicios", es decir, si demuestra que no existe relación de causalidad entre la infracción del RGPD y los perjuicios sufridos por la persona física. Aquí cabria incluir como causas de exoneración la fuerza mayor y la actuación exclusiva de la víctima, y cualquier criterio de imputación objetiva que rompa el nexo causal entre la infracción del RGPD y el daño.

2.2.6 El temor a un potencial uso indebido de los datos personales por terceros constituye un daño moral

El tribunal remitente pregunta si el artículo 82.1 RGPD debe interpretarse en el sentido de que el temor que experimenta un interesado a un potencial uso indebido de sus datos personales por terceros a raíz de una infracción del RGPD puede constituir, por sí solo, un "daño o perjuicio inmaterial" a los efectos de la mencionada disposición.

El TJUE subraya que el artículo 82.1 RGPD no distingue entre los supuestos en los que los daños y perjuicios inmateriales que alega el interesado están relacionados con un uso indebido de sus datos personales por terceros que ya se ha producido en la fecha de la demanda indemnizatoria, de los supuestos en los que esos daños y perjuicios inmateriales están relacionados con el *temor que experimenta ese interesado a que tal uso pueda producirse en el futuro*. Por consiguiente, el artículo 82.1 RGPD no excluye que el concepto de daños y perjuicios inmateriales incluya una situación en la que el interesado invoca su temor a que sus datos personales sean objeto de uso indebido en el futuro por parte de terceros como consecuencia de la infracción que se ha cometido del RGPD. Esta interpretación se ve corroborada por el considerando 146 RGPD, el cual declara que "el concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del" TJUE.

No obstante, el TJUE también manifiesta que un interesado afectado por una infracción del RGPD que haya tenido consecuencias negativas para él, debe demostrar que estas consecuencias constituyen daños y perjuicios inmateriales, en el sentido del artículo 82 RGPD. En particular, el juez nacional deberá comprobar que ese temor puede considerarse fundado, habida cuenta de las circunstancias específicas del caso y del interesado.

A la luz de las consideraciones anteriores, el TJUE responde a la cuestión prejudicial que el artículo 82.1 RGPD debe interpretarse en el sentido de que el temor que experimenta un interesado a un potencial uso indebido de sus datos personales por terceros a raíz de una infracción del RGPD puede constituir, por sí solo, un "daño o perjuicio inmaterial" a los efectos de la mencionada disposición.

Comentario: Según el TJUE, es un daño moral indemnizable la inquietud, ansiedad y temor del interesado acerca de un eventual futuro uso indebido de los datos personales, cuando ese uso indebido no se ha acreditado y el interesado no ha sufrido ningún otro daño. El temor a un uso indebido de datos personales puede provenir de un ciberataque, pero también de la entrega, por parte de un trabajador del responsable

del tratamiento, de un documento con datos personales a un tercero no autorizado que ha podido hacer copias antes de devolverlo[5].

Por tanto, se permite una acción por daño moral autónomo, sin necesidad de acreditar ningún daño material. Si el dato ha sido indebidamente utilizado y eso tiene consecuencias económicas, habrán de indemnizarse tanto el daño moral como el patrimonial. Por ejemplo, el daño patrimonial consiste en no poder acceder a créditos o a productos o servicios concretos por la revelación no autorizada de datos financieros.

Ahora bien, corresponde al demandante demostrar la existencia de tal daño moral, sin que un riesgo puramente hipotético de un uso indebido por un tercero no autorizado pueda dar lugar a indemnización. 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.

La violación de los preceptos del RGPD no produce necesariamente un daño moral solo porque genere al interesado un mero sentimiento de desagrado por el incumplimiento del RGPD. Si, por ejemplo, un responsable del tratamiento no coopera con una autoridad de control (art. 31 RGPD), se producirá in incumplimiento del RGPD, pero dicho incumplimiento, por sí solo, no equivale a un daño moral por la mera contravención de la ley. Una indemnización así podría suponer una indemnización sin daño, que, según el TJUE, no se contempla en el supuesto del artículo 82 RGPD. Por ende, el incumplimiento del RGPD tiene que ocasionar un daño al interesado distinto del mero desagrado ante la contravención de la ley.

La cierto es que doctrina del TJUE brinda mayor capacidad a los interesados para buscar una compensación por preocupaciones relacionadas con la seguridad de los datos personales. Ahora bien, la doctrina plantea desafíos en la práctica, al ser difícil determinar los criterios para cuantificar el alcance de dicho daño inmaterial. En buena lógica, la cuantía de la indemnización debería depender de la *gravedad de la lesión efectivamente producida* (art. 9.3 Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen). Así, habrá de tenerse en cuenta el tipo de dato personal afectado, pues la violación de la seguridad de algunos datos puede causar daños más importantes, como discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación o pérdida de confidencialidad. No es lo mismo que la comunicación no autorizada afecte al número de la seguridad social que a los datos de salud o al usuario y contraseña de la aplicación bancaria. También importa el tiempo durante el cual el dato estuvo accesible y el número más o menos amplio de potenciales terceros que pueden usar indebidamente los datos.

[5] STJUE de 25 de enero de 2024, asunto C-687/21, *BL y MediaMarktSaturm.*

3. ASUNTO C-667/21

3.1. Hechos

El *MDK Nordrhein* (en adelante, MDK) es un organismo de Derecho público que, como servicio médico de cajas de seguro de enfermedad, tiene por función legal emitir informes médicos con el fin de disipar dudas relativas a la incapacidad laboral de las personas aseguradas en las cajas de seguro obligatorio de enfermedad comprendidas en su ámbito de competencia, incluso cuando esos informes se refieren a sus propios empleados.

En tal caso, solo los miembros de una unidad especial, denominada "unidad de casos especiales", están autorizados a tratar los datos denominados "sociales" de ese empleado, utilizando un dominio bloqueado del sistema informático de ese organismo, y a acceder a los archivos digitales, tras la finalización del expediente relativo al informe pericial. En particular, solo un número limitado de trabajadores autorizados, incluidos algunos trabajadores del servicio informático, tendrán acceso a dichos datos.

El demandante en el litigio principal trabajó en el servicio informático del MDK antes de que se le concediera una incapacidad laboral por razones médicas. Al término del semestre durante el cual ese organismo, como empleador, continuó retribuyéndole, la caja de seguro obligatorio de enfermedad a la que estaba afiliado comenzó a pagarle prestaciones por enfermedad.

Esta caja solicitó entonces al MDK que emitiera un informe pericial sobre la incapacidad laboral del demandante en el litigio principal. Un médico que trabajaba en la "unidad de casos especiales" del MDK emitió el informe pericial, recabando, en particular, información del médico de cabecera del demandante en el litigio principal. Cuando su médico de cabecera le informó de ello, se puso en contacto con uno de sus compañeros de trabajo del servicio informático y le pidió que tomara fotografías del informe pericial que figuraba en los archivos digitales del MDK y que se las enviara posteriormente.

Al considerar que, de este modo, su empleador había tratado datos relativos a su salud ilícitamente, el demandante en el litigio principal reclamó a su empleador que le abonara una indemnización por importe de 20.000 euros, reclamación que fue rechazada por el MDK.

Posteriormente, el demandante presentó una demanda ante el Tribunal de lo Laboral de *Düsseldorf* en la que solicitaba, sobre la base del artículo 82.1 RGPD, que se condenara al MDK a reparar los daños y perjuicios que afirmaba haber sufrido como consecuencia del tratamiento de datos personales así efectuado. Alegaba, por una parte, que el informe pericial en cuestión debería haber sido realizado por otro servicio médico para evitar que sus compañeros de trabajo tuvieran acceso a datos relativos a su salud y, por otra, que las medidas de seguridad en torno al archivo del dictamen relativo a ese informe pericial eran insuficientes. Asimismo, sostenía que ese

tratamiento constituía una infracción de las normas que protegen tales datos y que le había ocasionado daños y perjuicios tanto inmateriales como materiales.

Al haber sido desestimadas sus pretensiones en primera instancia, el demandante interpuso recurso de apelación ante el Tribunal Regional de lo Laboral de *Düsseldorf,* que también desestimó su recurso. A continuación, interpuso un recurso de casación ante el Tribunal Supremo de lo Laboral, que decidió suspender el procedimiento y plantear al TJUE una serie de cuestiones prejudiciales, de las que vamos a seleccionar solo las que nos interesan para este trabajo.

3.2. Doctrina del TJUE

3.2.1. La indemnización del artículo 82 RGPD no tiene una función punitiva

El tribunal remitente desea saber si el artículo 82.1 RGPD debe interpretarse en el sentido de que el derecho a indemnización contemplado en esa disposición cumple no solo una función compensatoria, sino también una función disuasoria o punitiva, y, en caso afirmativo, si esta última debe tenerse en cuenta eventualmente al fijar el importe de la indemnización por daños y perjuicios concedida como reparación de un daño inmaterial sobre la base de esa disposición.

Según el TJUE, el artículo 82 RGPD no tiene una función punitiva, sino compensatoria, a diferencia de otras disposiciones como los artículos 83 y 84 RGPD, que tienen esencialmente una finalidad punitiva, puesto que permiten, respectivamente, imponer multas administrativas y otras sanciones. Si el derecho a indemnización contemplado en el artículo 82.1 RGPD no cumple una función disuasoria, ni siquiera punitiva, la gravedad de la infracción del RGPD que haya causado los daños y perjuicios en cuestión no puede influir en el importe de la indemnización concedida en virtud de dicha disposición, ni siquiera cuando los daños y perjuicios no sean materiales, sino inmateriales. De ello se deduce que ese importe no puede fijarse en una cuantía que exceda de la compensación completa de ese perjuicio.

En consecuencia, el TJUE responde a la cuestión prejudicial que el artículo 82.1 RGPD debe interpretarse en el sentido de que el derecho a indemnización contemplado en esa disposición cumple una función compensatoria, dado que una reparación pecuniaria basada en dicha disposición debe permitir compensar íntegramente los daños y perjuicios sufridos concretamente como consecuencia de la infracción del RGPD, y no una función disuasoria o punitiva.

Comentario: Algunas directivas contemplan expresamente indemnizaciones de carácter disuasorio, que están concebidas como sanciones. Así, por ejemplo, el artículo 25 de la Directiva 2006/54/CE del Parlamento Europeo y del Consejo, de 5 de julio de 2006, relativa a la aplicación del principio de igualdad de oportunidades e igualdad de trato entre hombres y mujeres en asuntos de empleo y ocupación. También el artículo 28 de la Directiva 2004/109/CE, de 15 de diciembre de 2004, sobre la armonización

de los requisitos de transparencia relativos a la información sobre los emisores cuyos valores se admiten a negociación en un mercado regulado. En España, la indemnización tiene una función punitiva en algunos ámbitos (arts. 576.1 LEC y 20 LCS). Pero, según el TJUE, el artículo 82 RGPD escapa de esta función punitiva, que es entregada a los artículos 83 y 84 RGPD, por lo que la indemnización que regula solo puede servir para devolver al interesado a la situación en la que estaría de no haberse producido el daño, y no para más. Con todo, es chocante que se diga que la indemnización del artículo 82 RGPD no tiene funciones punitivas pero que se admita la indemnización por daños morales no ligados a daños materiales, indemnización que podría considerarse que tienen cierta función disuasoria.

3.2.2. El nacimiento de la responsabilidad del responsable del tratamiento está supeditado a la existencia de culpa

El tribunal remitente pregunta, por un lado, si el artículo 82 RGPD debe interpretarse en el sentido de que el nacimiento de la responsabilidad del responsable del tratamiento está supeditado a la existencia de culpa por parte de este y, por otro lado, si el grado de culpa debe tenerse en cuenta al fijar el importe de la indemnización por daños y perjuicios.

Según el TJUE, del análisis conjunto de las diferentes disposiciones del artículo 82 RGPD se desprende que este artículo establece un régimen de responsabilidad por culpa en el que la carga de la prueba recae sobre el responsable del tratamiento. Esta interpretación se ve corroborada por el contexto en el que se inscribe ese artículo 82 y por los objetivos perseguidos por el legislador de la Unión a través del RGPD.

A este respecto, el TJUE señala que del tenor de los artículos 24 y 32 RGPD se desprende que estas disposiciones 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 los datos personales. El carácter adecuado de tales medidas debe evaluarse de manera concreta, examinando si esas medidas han sido aplicadas por el responsable del tratamiento teniendo en cuenta los diferentes criterios contemplados en dichos artículos y las necesidades de protección de datos específicamente inherentes al tratamiento en cuestión, así como a los riesgos derivados de este. Pues bien, tal obligación quedaría en entredicho si el responsable del tratamiento estuviera obligado, a continuación, a reparar cualquier daño causado por un tratamiento realizado infringiendo el RGPD.

A juicio del TJUE, de los considerandos 4 a 8 RGPD se desprende que el RGPD tiene por objeto establecer un equilibrio entre los intereses de los responsables del tratamiento de datos personales y los derechos de las personas cuyos datos se tratan. El objetivo perseguido es permitir el desarrollo de la economía digital, garantizando al mismo tiempo un elevado nivel de protección de las personas. La finalidad es, por tanto, la ponderación de los intereses del responsable del tratamiento y de las personas cuyos datos personales se tratan. Así, un mecanismo de responsabilidad por

culpa acompañado de una inversión de la carga de la prueba, como establece el artículo 82 RGPD, permite precisamente garantizar tal equilibrio.

Entiende el TJUE que no sería conforme con el objetivo de tal protección elevada optar por una interpretación según la cual los interesados que han sufrido daños y perjuicios como consecuencia de una infracción del RGPD deben soportar la carga de probar no solo la existencia de esa infracción y de los daños y perjuicios que se derivan para ellos de esa infracción, sino también la existencia de culpa, por intencionalidad o negligencia, por parte del responsable del tratamiento, o incluso el grado de culpa, aun cuando el artículo 82 RGPD no formule tales requisitos. Por otra parte, un régimen de responsabilidad objetiva no garantizaría la consecución del objetivo de seguridad jurídica perseguido por el legislador, como se desprende del considerando 7 RGPD.

Finalmente, el TJUE señala que, habida cuenta de su función compensatoria, el artículo 82 RGPD no exige que la gravedad de la infracción del RGPD, que se presume que el responsable del tratamiento ha cometido, sea tenida en cuenta al fijar el importe de la indemnización por daños y perjuicios concedida como reparación de un daño inmaterial sobre la base de esa disposición, sino que exige que ese importe se fije de manera que se compensen íntegramente los daños y perjuicios sufridos concretamente como consecuencia de la infracción del RGPD.

En suma, el TJUE responde a la cuestión prejudicial que el artículo 82 RGPD debe interpretarse en el sentido de que, por una parte, el nacimiento de la responsabilidad del responsable del tratamiento está supeditado a la existencia de culpa por parte de este, la cual se presume, a menos que este demuestre que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios, y, por otra parte, no exige que el grado de culpa se tenga en cuenta al fijar el importe de la indemnización.

Comentario: El artículo 82 RGPD solo exige para que nazca el derecho a indemnización una infracción del RGPD ligada a la producción de unos daños. No hay ninguna referencia en el artículo 82 RGPD a la culpa del responsable como requisito para que nazca el derecho a indemnización. Con todo, según el TJUE, el artículo 82 RGPD condiciona el nacimiento de la responsabilidad del responsable del tratamiento a que este haya infringido el RGPD con culpa. En otros lugares, el TJUE ha entendido que el responsable comete una infracción con culpa cuando no podía ignorar el carácter infractor de su conducta, tuviera o no conciencia de infringir las disposiciones del RGPD[6].

El TJUE emite esta doctrina en un caso en el que el responsable del tratamiento ha podido infringir alguna obligación del RGPD en cuanto al tratamiento y la seguridad de los datos personales, pero en el que el acceso o comunicación no autorizada de los datos parece estar provocada por la propia actuación del interesado. Con la introducción de la culpa como criterio de imputación de responsabilidad el TJUE parece querer evitar que la mera infracción del RGPD haga nacer el derecho a indemnización,

[6] STJUE de 5 de diciembre del 2023, asunto C-683-2, *Nacionalinis y Valstybinė* (EU:C:2023:949).

cuando el acto dañoso ha sido causado por la propia actuación del interesado. Con todo, yo creo que para resolver este problema no es necesario la introducción de la culpa como criterio de imputación de responsabilidad, y el asunto se podría solucionar con el artículo 82.3 RGPD, pues el responsable podría alegar que "no es modo alguno responsable" del hecho que ha producido los daños, los cuales han sido causados por la actuación del interesado. En mi opinión, 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.

Finalmente, el TJUE afirma que la incidencia del grado de culpa del responsable del tratamiento no puede influir en la cuantificación de la indemnización, de forma que no es posible modular a la baja su cuantía atendiendo al menor grado de negligencia del responsable. En realidad, no se trata de graduar la indemnización según la mayor o menor gravedad de la conducta del responsable del tratamiento, sino según la mayor o menor gravedad del daño que dicha conducta causa al interesado. En este sentido, el artículo 9 LPDH se refiere a "la gravedad de la lesión efectivamente producida", y no a la culpa o conducta del agente.

4. BIBLIOGRAFÍA

BASOZABAL ARRUE, X., *La responsabilidad extracontractual objetiva*, BOE, 2015.

CARRASCO PERERA, Á., "Responsable y encargado del tratamiento", *Publicaciones GA-P*, 2024.

DE MIGUEL ASENSIO, P. A., "Requisitos del derecho a indemnización en el Reglamento General de Protección de Datos", *La Ley Unión Europea*, 115, 2023.

GARCÍA HERNÁNDEZ, Á., "Responsabilidad civil de encargados y responsables del tratamiento de datos en el reglamento UE de protección de datos", *Revista CESCO*, 41, 2022.

GELLERT, R.M., "Understanding data protection as risk regulation", *Journal of Internet Law,* 3, 2015.

NEMITZ, P., "Fines under the GDPR", *Data Protection and Privacy: The Internet of Bodies* (Leenes, R., van Brakel, R., Gutwirth, S. y De Hert, P.), Hart Publishing, 2019.

O'DELL, E., "Compensation for Breach of the General Data Protection Regulation", 40, Dublin *University Law Journal*, 2017.

PANTALEÓN PRIETO, F., "Comentario al artículo 1902 CC", *Comentarios al Código Civil*, Ministerio de Justicia, 2015.

RUBÍ PUIG, A., "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil*, 5, 2018.

SANTOS MORÓN, M.ª C., "Tratamiento de datos, sujetos implicados y responsabilidad proactiva", en *Protección de datos personales* (Coords. Isabel González Pacanowska y Margarita Castilla Barea), Tirant lo Blanch, 2020.

TORRES LANA, J.A., "Los daños punitivos y su posible trasplante al sistema jurídico español", *Cuestiones clásicas y actuales del Derecho de daños* (coord. Joaquín Ataz López), Aranzadi, 2021.

VAN ALSENOY, B., "Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation", *JIPITEC,* 3, 2016.