Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Sala Tercera)

de 14 de diciembre de 2023 *

«Procedimiento prejudicial — Protección de las personas físicas en lo que respecta al tratamiento de datos personales — Reglamento (UE) 2016/679 — Artículo 5 — Principios relativos a dicho tratamiento — Artículo 24 — Responsabilidad del responsable del tratamiento — Artículo 32 — Medidas adoptadas para garantizar la seguridad del tratamiento — Apreciación del carácter apropiado de tales medidas — Alcance del control jurisdiccional — Práctica de la prueba — Artículo 82 — Derecho a indemnización y responsabilidad — Eventual exoneración de responsabilidad del responsable del tratamiento en caso de violación de datos cometida por terceros — Demanda de indemnización por daños y perjuicios inmateriales basada en el temor a un uso indebido de datos personales»

En el asunto C-340/21,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por el Varhoven administrativen sad (Tribunal Supremo de lo Contencioso-Administrativo, Bulgaria), mediante resolución de 14 de mayo de 2021, recibida en el Tribunal de Justicia el 2 de junio de 2021, en el procedimiento entre

VB

y

Natsionalna agentsia za prihodite,

EL TRIBUNAL DE JUSTICIA (Sala Tercera),

integrado por la Sra. K. Jürimäe, Presidenta de Sala, y los Sres. N. Piçarra, M. Safjan, N. Jääskinen (Ponente) y M. Gavalec, Jueces;

Abogado General: Sr. G. Pitruzzella;

Secretario: Sr. A. Calot Escobar;

habiendo considerado los escritos obrantes en autos;

consideradas las observaciones presentadas:

– en nombre de la Natsionalna agentsia za prihodite, por el Sr. R. Spetsov;

* Lengua de procedimiento: búlgaro.

– en nombre del Gobierno búlgaro, por las Sras. M. Georgieva y L. Zaharieva, en calidad de agentes;

– en nombre del Gobierno checo, por los Sres. O. Serdula, M. Smolek y J. Vláčil, en calidad de agentes;

– en nombre de Irlanda, por la Sra. M. Browne, Chief State Solicitor, el Sr. A. Joyce, la Sra. J. Quaney y el Sr. M. Tierney, en calidad de agentes, asistidos por el Sr. D. Fennelly, BL;

– en nombre del Gobierno italiano, por la Sra. G. Palmieri, en calidad de agente, asistida por el Sr. E. De Bonis, avvocato dello Stato;

– en nombre del Gobierno portugués, por las Sras. P. Barros da Costa, A. Pimenta, M. J. Ramos y C. Vieira Guerra, en calidad de agentes;

– en nombre de la Comisión Europea, por los Sres. A. Bouchagiar y H. Kranenborg y la Sra. N. Nikolova, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 27 de abril de 2023;

dicta la siguiente

Sentencia

1 La presente petición de decisión prejudicial tiene por objeto la interpretación de los artículos 5, apartado 2, 24, 32 y 82, apartados 1 a 3, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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 (Reglamento general de protección de datos) (DO 2016, L 119, p. 1; en lo sucesivo, «RGPD»).

2 Esta petición se ha presentado en el contexto de un litigio entre VB, una persona física, y la Natsionalna agentsia za prihodite (Agencia Nacional de Recaudación, Bulgaria; en lo sucesivo, «NAP») en relación con la indemnización por los daños y perjuicios inmateriales que dicha persona afirma haber sufrido como consecuencia de un supuesto incumplimiento por parte de dicha autoridad pública de las obligaciones legales que le incumben en su condición de responsable del tratamiento de datos personales.

Marco jurídico

3 Los considerandos 4, 10, 11, 74, 76, 83, 85 y 146 del RGPD están redactados como sigue:

«(4) […] El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta [de los Derechos Fundamentales de la Unión Europea] conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, […] el derecho a la tutela judicial efectiva y a un juicio justo […]

[…]

(10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión [Europea], el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. […]

(11) La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal […]

[…]

(74) Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

[…]

(76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

[…]

(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

[…]

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida […] notificar la violación de la seguridad de los datos personales a la autoridad de control […]

[…]

(146) El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento. El responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios. El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros. 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. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos. […]»

4 El artículo 4 de dicho Reglamento, con el título «Definiciones», dispone:

«A efectos del presente Reglamento se entenderá por:

1) “datos personales”: toda información sobre una persona física identificada o identificable (“el interesado”); […]

2) “tratamiento”: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no […]

[…]

7) “responsable del tratamiento” o “responsable”: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; […]

[…]

10) “tercero”: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

[…]

12) “violación de la seguridad de los datos personales”: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

[…]».

5 El artículo 5 del citado Reglamento, titulado «Principios relativos al tratamiento», establece:

«1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado (“licitud, lealtad y transparencia”);

[…]

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (“integridad y confidencialidad”).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (“responsabilidad proactiva”).»

6 A tenor del artículo 24 del mismo Reglamento, que lleva por título «Responsabilidad del responsable del tratamiento»:

«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.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.»

7 El artículo 32 del RGPD, con el título «Seguridad del tratamiento», dispone:

«1. 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, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

[…]»

8 El artículo 79 del RGPD, titulado «Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento», establece en su apartado 1:

«Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.»

9 El artículo 82 de dicho Reglamento, que lleva por título «Derecho a indemnización y responsabilidad», establece en sus apartados 1 a 3:

«1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

2. 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 presente Reglamento. […]

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.»

Litigio principal y cuestiones prejudiciales

10 La 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, apartado 7, del RGPD.

11 El 15 de julio de 2019, los medios de comunicación informaron de que se había producido un acceso no autorizado al sistema informático de la NAP y que, a raíz de este ciberataque, se habían publicado en Internet datos personales almacenados en dicho sistema.

12 Más de seis millones de personas físicas, de nacionalidad búlgara y extranjera, se vieron afectadas por estos hechos. Cientos de ellas, como la demandante en el litigio principal, ejercieron acciones contra la NAP reclamando una indemnización por los daños y perjuicios inmateriales supuestamente derivados de la comunicación de sus datos personales.

13 En este contexto, la demandante en el litigio principal interpuso ante el Administrativen sad Sofia-grad (Tribunal de lo Contencioso-Administrativo de Sofía, Bulgaria) una demanda mediante la que solicitaba que la NAP le abonara la cantidad de 1 000 levas búlgaras (BGN) (aproximadamente 510 euros) en concepto de indemnización por daños y perjuicios, en virtud del artículo 82 del RGPD y de determinadas disposiciones del Derecho búlgaro. En apoyo de esta demanda, la demandante alegó que había sufrido un perjuicio inmaterial derivado de la violación de la seguridad de los datos personales, en el sentido del artículo 4, apartado 12, del RGPD, más concretamente, una violación de la seguridad derivada del incumplimiento por parte de la NAP de las obligaciones que le incumbían, en particular, en virtud de los artículos 5, apartado 1, letra f), 24 y 32 de dicho Reglamento. 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.

14 En su defensa, la NAP alegó, en primer término, que la demandante en el litigio principal no le había solicitado información sobre los datos concretos que habían sido divulgados. A continuación, la NAP presentó documentos para demostrar 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, según la NAP, no existía relación de causalidad entre el perjuicio inmaterial alegado y la citada violación. Por último, la NAP alegó 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.

15 Mediante resolución de 27 de noviembre de 2020, el Administrativen sad Sofia-grad (Tribunal de lo Contencioso-Administrativo de Sofía) desestimó la demanda de la demandante en el litigio principal. Dicho órgano jurisdiccional 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 en el litigio principal no había demostrado que la NAP no hubiera adoptado medidas de seguridad. Por otro lado, estimó que la demandante no había sufrido daño o perjuicio inmaterial alguno que diera derecho a indemnización.

16 La demandante en el litigio principal interpuso un recurso de casación contra la mencionada resolución ante el Varhoven administrativen sad (Tribunal Supremo de lo Contencioso-Administrativo, Bulgaria), que es el órgano jurisdiccional remitente en el presente asunto. En apoyo de su recurso de casación, dicho Tribunal 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. Además, la demandante en el litigio principal alega que el temor a que sus datos personales puedan utilizarse indebidamente en el futuro constituye un perjuicio inmaterial real y no hipotético. En su escrito de contestación, la NAP rebate cada una de estas alegaciones.

17 El órgano jurisdiccional remitente, de entrada, considera posible que la constatación de que se ha producido una violación de la seguridad de los datos personales permita, por sí sola, concluir que las medidas adoptadas por el responsable del tratamiento de esos datos no eran «apropiadas», en el sentido de los artículos 24 y 32 del RGPD.

18 Sin embargo, en el supuesto de que esta constatación sea insuficiente para llegar a dicha conclusión, el órgano jurisdiccional remitente se pregunta, por un lado, cuál es el alcance del control que los jueces nacionales deben llevar a cabo para evaluar el carácter apropiado de las medidas de que se trate y, por otro lado, cuáles son las normas relativas a la práctica de la prueba que deben aplicarse en este contexto, tanto en lo que respecta a la carga de la prueba como en lo que respecta a los medios de prueba, en particular cuando se ejercita ante dichos jueces una acción de indemnización al amparo del artículo 82 del citado Reglamento.

19 A continuación, el órgano jurisdiccional remitente desea saber si, a la luz del artículo 82, apartado 3, del mencionado Reglamento, el hecho de que la violación de la seguridad de los datos personales resulte de un acto cometido por terceros, en este caso, un ciberataque, constituye un factor que exonera sistemáticamente al responsable del tratamiento de esos datos de responsabilidad por el perjuicio causado al interesado.

20 Por último, el mencionado órgano jurisdiccional se pregunta si el temor de una persona a que sus datos personales puedan ser objeto de un uso indebido en el futuro, en el presente asunto a raíz de un acceso no autorizado a estos datos y de su comunicación por ciberdelincuentes, puede constituir, por sí solo, un «daño o perjuicio inmaterial» en el sentido del artículo 82, apartado 1, del RGPD. En caso afirmativo, dicha persona no tendría que demostrar que, con anterioridad a su acción de indemnización, se produjo un uso ilícito de esos datos, como una usurpación de su identidad, por parte de terceros.

21 En estas circunstancias, el Varhoven administrativen sad (Tribunal Supremo de lo Contencioso-Administrativo) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Deben interpretarse los artículos 24 y 32 del [RGPD] en el sentido de que basta una comunicación no autorizada de datos personales o un acceso no autorizado a datos personales, a efectos del artículo 4, punto 12, [de dicho Reglamento,] por personas que no son empleados de la administración del responsable del tratamiento y no están sometidas al control de este, para considerar que las medidas técnicas y organizativas adoptadas no eran apropiadas?

2) En caso de respuesta negativa a la primera cuestión, ¿qué objeto y alcance ha de tener el control judicial de legalidad al examinar si las medidas técnicas y organizativas adoptadas por el responsable del tratamiento son apropiadas con arreglo al artículo 32 del [RGPD]?

3) En caso de respuesta negativa a la primera cuestión, ¿debe interpretarse el principio de responsabilidad proactiva de los artículos 5, apartado 2, y 24 [del RGPD] en relación con el considerando 74 de [este Reglamento] en el sentido de que, en el marco de una acción ejercitada al amparo del artículo 82, apartado 1, [del mencionado Reglamento,] incumbe al responsable del tratamiento la carga de probar que las medidas técnicas y organizativas son apropiadas con arreglo al artículo 32 [de ese mismo] Reglamento?

¿Puede considerarse que un informe pericial ordenado por el juez es un medio de prueba necesario y suficiente para determinar si las medidas técnicas y organizativas adoptadas por el responsable del tratamiento eran apropiadas en un caso como el presente, en el que el acceso y la comunicación no autorizados de datos personales se produjeron a consecuencia de un "ciberataque"?

4) ¿Debe interpretarse el artículo 82, apartado 3, del [RGPD] en el sentido de que la comunicación o el acceso no autorizados a datos personales en el sentido del artículo 4, punto 12, del [RGPD], como en el presente caso, mediante un "ciberataque", por personas que no son empleados de la administración del responsable y que no están sometidas al control de este, constituye un hecho del cual no debe responder en modo alguno el responsable del tratamiento, lo que implica su total exoneración de responsabilidad?

5) ¿Debe interpretarse el artículo 82, apartados 1 y 2, [del RGPD,] en relación con los considerandos 85 y 146 [de dicho RGPD,] en el sentido de que, en un caso como el presente, en el que se ha producido una violación de la seguridad de los datos personales consistente en el acceso no autorizado a ciertos datos personales mediante un "ciberataque" y la difusión de dichos datos, los meros temores, miedos y preocupaciones del interesado respecto a un posible uso indebido de sus datos personales en el futuro están comprendidos en el concepto de daños inmateriales, que ha de ser interpretado en sentido amplio, y fundamentan una pretensión indemnizatoria, aunque no se haya constatado tal uso indebido o el interesado no haya sufrido ningún otro perjuicio?»

Sobre las cuestiones prejudiciales

Primera cuestión prejudicial

22 Mediante su primera cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si los artículos 24 y 32 del 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», a los efectos del artículo 4, punto 10, del mencionado Reglamento, 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.

23 Con carácter preliminar, procede recordar que, según reiterada jurisprudencia, el tenor de una disposición de Derecho de la Unión que, como los artículos 24 y 32 del RGPD, no contenga una remisión expresa al Derecho de los Estados miembros para determinar su sentido y su alcance debe normalmente ser objeto de una interpretación autónoma y uniforme en toda la Unión, que debe buscarse, en particular, teniendo en cuenta el tenor de la disposición en cuestión, los objetivos perseguidos por esta y el contexto en el que se inscribe [véanse, en este sentido, la sentencias de 18 de enero de 1984, Ekro, 327/82, EU: C:1984:11, apartado 11; de 1 de octubre de 2019, Planet49, C-673/17, EU:C:2019:801, apartados 47 y 48, y de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370, apartado 29].

24 En primer lugar, por lo que respecta al tenor de las disposiciones pertinentes, procede señalar que el artículo 24 del RGPD establece una obligación general, que recae sobre el responsable del tratamiento de datos personales, de aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que dicho tratamiento es conforme con el mencionado Reglamento.

25 A estos efectos, el citado artículo 24 enumera, en su apartado 1, una serie de criterios que deben tenerse en cuenta para evaluar el carácter apropiado de tales medidas, a saber, 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. Esta disposición añade que dichas medidas deberán revisarse y actualizarse cuando sea necesario.

26 Desde esta perspectiva, el artículo 32 del RGPD especifica cuáles son las obligaciones del responsable y de un eventual encargado del tratamiento en relación con la seguridad de este. De esta forma, el apartado 1 del citado artículo dispone que estos deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos mencionados en el apartado anterior de la presente sentencia, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento de que se trate.

27 Asimismo, el apartado 2 de dicho artículo establece que, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

28 Además, tanto el artículo 24, apartado 3, como el artículo 32, apartado 3, del mencionado Reglamento indican que el responsable o el encargado del tratamiento pueden demostrar que han cumplido los requisitos del apartado 1 de cada uno de esos artículos basándose en que se han adherido a un código de conducta aprobado o a un mecanismo de certificación aprobado, con arreglo a lo dispuesto en los artículos 40 y 42 de dicho Reglamento.

29 La referencia que figura en el artículo 32, apartados 1 y 2, del RGPD, a «un nivel de seguridad adecuado al riesgo» y a un «nivel de seguridad adecuado» pone de manifiesto que este Reglamento instaura un régimen de gestión de riesgos y que en modo alguno pretende eliminar los riesgos de violación de la seguridad de los datos personales.

30 Así, del tenor de los artículos 24 y 32 del 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 la seguridad de los datos personales. El carácter apropiado de tales medidas debe evaluarse en cada caso concreto, examinando si el responsable ha adoptado esas medidas teniendo en cuenta los diferentes criterios establecidos en los mencionados artículos y las necesidades de protección de datos específicamente inherentes al tratamiento de que se trate y a los riesgos que conlleva.

31 Por consiguiente, los artículos 24 y 32 del RGPD no pueden entenderse en el sentido de que una comunicación no autorizada de datos personales o un acceso no autorizado a dichos datos por parte de un tercero basten para concluir que las medidas adoptadas por el responsable del tratamiento no eran apropiadas, en el sentido de esas disposiciones, sin siquiera permitir a este último aportar la prueba en contrario.

32 Tal interpretación se impone tanto más cuanto que el artículo 24 del RGPD establece expresamente que el responsable del tratamiento debe poder demostrar la conformidad con dicho Reglamento de las medidas que ha adoptado, posibilidad de la que se vería privado si se admitiera una presunción *iuris et de iure*.

33 En segundo lugar, consideraciones de orden contextual y teleológico corroboran esta interpretación de los artículos 24 y 32 del RGPD.

34 En lo que se refiere, por un lado, al contexto en el que se inscriben estos dos artículos, procede señalar que del artículo 5, apartado 2, del RGPD se desprende que el responsable del tratamiento debe poder demostrar que ha respetado los principios relativos al tratamiento de datos personales establecidos en el apartado 1 del mismo artículo. Esta obligación se recoge y desarrolla en los artículos 24, apartados 1 y 3, y 32, apartado 3, del mencionado Reglamento, en lo que se refiere a la obligación de adoptar medidas técnicas y organizativas para proteger estos datos en el tratamiento llevado a cabo por dicho responsable. Pues bien, esta obligación de demostrar que esas medidas son apropiadas carecería de sentido si el responsable del tratamiento estuviera obligado a impedir toda violación de la seguridad de dichos datos.

35 Además, el considerando 74 del RGPD pone de relieve la importancia de que el responsable del tratamiento esté obligado a aplicar medidas oportunas y eficaces y pueda demostrar la conformidad de las actividades de tratamiento con dicho Reglamento, incluida la eficacia de las medidas, que deben tener en cuenta criterios relacionados con las características del tratamiento en cuestión y con el riesgo que presente este, que también se establecen en sus artículos 24 y 32.

36 Asimismo, según el considerando 76 del mencionado Reglamento, la probabilidad y la gravedad del riesgo dependen de las especificidades del tratamiento en cuestión y dicho riesgo debe ponderarse sobre la base de una evaluación objetiva.

37 Por otra parte, del artículo 82, apartados 2 y 3, del RGPD se desprende que, si bien un responsable del tratamiento es responsable del daño causado por un tratamiento que constituya una infracción de dicho Reglamento, queda exonerado de responsabilidad si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

38 Por otro lado, la interpretación expuesta en el apartado 31 de la presente sentencia también se ve respaldada por el considerando 83 del RGPD, que establece, en su primera frase, que, «a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos». De este modo, 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.

39 Por cuantas razones anteceden, procede responder a la primera cuestión prejudicial que los artículos 24 y 32 del 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», a los efectos del artículo 4, punto 10, del mencionado Reglamento, 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 24 y 32.

Segunda cuestión prejudicial

40 Mediante su segunda cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si el artículo 32 del 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, en particular teniendo en cuenta los riesgos vinculados al tratamiento de los datos.

41 A este respecto, procede recordar que, como se señala en la respuesta a la primera cuestión prejudicial, el artículo 32 del RGPD exige que el responsable y el encargado del tratamiento, según el caso, apliquen medidas técnicas y organizativas apropiadas a fin de garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta los criterios de apreciación mencionados en su apartado 1. Además, el apartado 2 de este artículo enumera, de manera no exhaustiva, una serie de factores que resultan pertinentes para evaluar el nivel de seguridad adecuado a los riesgos que presente el referido tratamiento.

42 Del citado artículo 32, apartados 1 y 2, se desprende que el carácter apropiado de tales medidas técnicas y organizativas debe apreciarse de manera escalonada. Por una parte, es preciso identificar los riesgos de violación de la seguridad de los datos personales que entrañe el tratamiento y sus posibles consecuencias para los derechos y libertades de las personas físicas. Esta apreciación debe llevarse a cabo en cada caso concreto, tomando en consideración cuál es la probabilidad de los riesgos identificados y la gravedad de estos. Seguidamente, debe comprobarse si las medidas adoptadas por el responsable del tratamiento se adaptan a estos riesgos, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento.

43 Es cierto que 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, apartado 1, del RGPD. No obstante, los órganos jurisdiccionales nacionales deben poder evaluar, en su complejidad, la apreciación realizada por el responsable del tratamiento y, de este modo, asegurarse de que las medidas adoptadas por este último son idóneas para garantizar tal nivel de seguridad.

44 De hecho, esta interpretación garantiza, por un lado, la eficacia de la protección de los datos personales que los considerandos 11 y 74 del citado Reglamento ponen de relieve y, por otro lado, el derecho a la tutela judicial efectiva frente a un responsable del tratamiento, tal como viene protegido por el artículo 79, apartado 1, de dicho Reglamento, en relación con el considerando 4 de este.

45 Por consiguiente, para controlar el carácter apropiado de las medidas técnicas y organizativas adoptadas con arreglo al artículo 32 del RGPD, un órgano jurisdiccional 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.

46 Un examen de este tipo requiere que se proceda a un análisis concreto tanto de la naturaleza como del contenido de las medidas que han sido adoptadas por el responsable del tratamiento, de la forma en la que se han aplicado dichas medidas y de sus efectos prácticos en el nivel de seguridad que este estaba obligado a garantizar, habida cuenta de los riesgos inherentes a ese tratamiento.

47 Por consiguiente, procede responder a la segunda cuestión prejudicial que el artículo 32 del 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.

Tercera cuestión prejudicial

Primera parte de la tercera cuestión prejudicial

48 Mediante la primera parte de su tercera cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si el principio de responsabilidad del responsable del tratamiento, enunciado en el artículo 5, apartado 2, del RGPD y desarrollado en el artículo 24 de este, debe interpretarse en el sentido de que, en el marco de una acción de indemnización basada en el artículo 82 del citado Reglamento, 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 del mencionado Reglamento.

49 A este respecto, procede recordar, en primer lugar, que el artículo 5, apartado 2, del RGPD establece un principio de responsabilidad en virtud del cual el responsable del tratamiento es responsable del respeto de los principios relativos al tratamiento de datos personales enunciados en el apartado 1 de ese artículo y estipula que este responsable debe ser capaz de demostrar la conformidad del tratamiento con dichos principios.

50 En particular, el responsable del tratamiento debe, de conformidad con los principios de integridad y de confidencialidad de los datos personales establecidos en el artículo 5, apartado 1, letra f), de dicho Reglamento, garantizar que estos datos son tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas y debe ser capaz de demostrar la conformidad con los referidos principios.

51 Asimismo, procede señalar que tanto el artículo 24, apartado 1, del RGPD, en relación con el considerando 74 de este, como el artículo 32, apartado 1, del mismo Reglamento obligan al responsable del tratamiento, para todo tratamiento de datos personales realizado por él mismo o por su cuenta, a aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

52 Del tenor de los artículos 5, apartado 2, 24, apartado 1, y 32, apartado 1, del RGPD se desprende inequívocamente que la carga de la prueba de que los datos personales se tratan de modo que se garantiza una seguridad adecuada, en el sentido de los artículos 5, apartado 1, letra f), y 32 de dicho Reglamento, incumbe al responsable del tratamiento en cuestión [véanse, por analogía, las sentencias de 4 de mayo de 2023, Bundesrepublik Deutschland (Buzón electrónico judicial), C-60/22, EU: C:2023:373, apartados 52 y 53, y de 4 de julio de 2023, Meta Platforms y otros (Condiciones generales del servicio de una red social), C-252/21, EU:C:2023:537, apartado 95].

53 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 de dicho Reglamento.

54 En segundo lugar, procede señalar que la anterior interpretación literal se ve corroborada si se toman en consideración los objetivos que persigue el RGPD.

55 Por un lado, dado que el nivel de protección a que se refiere el RGPD depende de las medidas de seguridad adoptadas por los responsables del tratamiento de datos personales, debe incitarse a estos, haciendo que recaiga en ellos la carga de demostrar el carácter apropiado de esas medidas, a hacer todo lo posible para evitar que se lleven a cabo operaciones de tratamiento no conformes con el citado Reglamento.

56 Por otro lado, si se considerase que la carga de la prueba relativa al carácter apropiado de las mencionadas medidas recae sobre los interesados, tal como se definen en el artículo 4, punto 1, del RGPD, de ello resultaría que el derecho a indemnización contemplado en el artículo 82, apartado 1, de este se vería privado de gran parte de su efecto útil, pese a que el legislador de la Unión pretendió reforzar tanto los derechos de esos interesados como las obligaciones de los responsables del tratamiento, a la vista de las disposiciones anteriores a dicho Reglamento, como indica su considerando 11.

57 Procede, en consecuencia, responder a la primera parte de la tercera cuestión prejudicial que el principio de responsabilidad del responsable del tratamiento, enunciado en el artículo 5, apartado 2, del RGPD y desarrollado en el artículo 24 de este, debe interpretarse en el sentido de que, en el marco de una acción de indemnización basada en el artículo 82 del citado Reglamento, 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 del mencionado Reglamento.

Segunda parte de la tercera cuestión prejudicial

58 Mediante la segunda parte de su tercera cuestión prejudicial, el órgano jurisdiccional remitente desea que se dilucide, en esencia, si el artículo 32 del 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.

59 A este respecto, es preciso recordar que, según reiterada jurisprudencia, a falta de normas de la Unión en la materia, corresponde al ordenamiento jurídico interno de cada Estado miembro configurar la regulación procesal de los recursos judiciales destinados a garantizar la salvaguardia de los derechos de los justiciables, en virtud del principio de autonomía procesal, a condición, sin embargo, de que dicha regulación no sea menos favorable que la que rige situaciones similares de carácter interno (principio de equivalencia) y de que no haga imposible en la práctica o excesivamente difícil el ejercicio de los derechos que confiere el ordenamiento jurídico de la Unión (principio de efectividad) [sentencia de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370, apartado 53 y jurisprudencia citada].

60 En el presente asunto, es preciso señalar que el RGPD no establece reglas relativas a la admisión y al valor probatorio de un medio de prueba, como es el peritaje judicial, que deben aplicar los jueces nacionales que conozcan de una acción de indemnización basada en el artículo 82 de dicho Reglamento y que deben apreciar, a la luz del artículo 32 del mismo Reglamento, el carácter apropiado de las medidas de seguridad que el responsable del tratamiento haya adoptado. Por consiguiente, de conformidad con lo expuesto en el apartado anterior de la presente sentencia y en ausencia de normas del Derecho de la Unión en la materia, corresponde al ordenamiento jurídico interno de cada Estado miembro establecer los tipos de acciones que permitan garantizar los derechos que confiere el citado artículo 82 a los justiciables y, en particular, las reglas relativas a los medios de prueba que permiten evaluar el carácter apropiado de dichas medidas en este contexto, siempre que se respeten los citados principios de equivalencia y efectividad [véanse, por analogía, las sentencias de 21 de junio de 2022, Ligue des droits humains, C-817/19, EU: C:2022:491, apartado 297, y de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370, apartado 54].

61 En el presente procedimiento, el Tribunal de Justicia no dispone de ningún elemento que le haga dudar de que se respeta el principio de equivalencia. No sucede lo mismo en lo que respecta a la conformidad con el principio de efectividad, en la medida en que el propio tenor de la segunda parte de la tercera cuestión prejudicial presenta el peritaje judicial como un «medio de prueba necesario y suficiente».

62 En particular, una regla procesal nacional en virtud de la cual es sistemáticamente «necesario» que los órganos jurisdiccionales nacionales ordenen un informe pericial podría vulnerar el principio de efectividad. En efecto, el recurso sistemático a dicho informe pericial puede resultar superfluo a la vista de las demás pruebas en poder del órgano jurisdiccional que conoce del asunto, en particular, como ha indicado el Gobierno búlgaro en sus observaciones escritas, habida cuenta de 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, puesto que las mencionadas medidas deben, de conformidad con el artículo 24, apartado 1, del RGPD, revisarse y actualizarse cuando sea necesario.

63 Además, como ha señalado la Comisión Europea en sus observaciones escritas, el principio de efectividad podría resultar vulnerado si el término «suficiente» se entendiera en el sentido de que un órgano jurisdiccional nacional debe deducir exclusiva o automáticamente de un informe pericial que las medidas de seguridad adoptadas por el responsable del tratamiento de que se trate son «apropiadas», en el sentido del artículo 32 del RGPD. La salvaguarda de los derechos conferidos por dicho Reglamento, a la que va orientado el principio de efectividad, y especialmente el derecho a la tutela judicial efectiva contra el responsable del tratamiento, reconocido en su artículo 79, apartado 1, exigen que un órgano jurisdiccional imparcial proceda a una apreciación objetiva del carácter apropiado de las medidas de que se trate, en lugar de limitarse a realizar tal deducción (véase, en este sentido, la sentencia de 12 de enero de 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, apartado 50).

64 Habida cuenta de las consideraciones anteriores, procede responder a la segunda parte de la tercera cuestión prejudicial que el artículo 32 del 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.

Cuarta cuestión prejudicial

65 Mediante su cuarta cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si el artículo 82, apartado 3, del RGPD debe interpretarse en el sentido de que el responsable del tratamiento está exonerado de la obligación de indemnizar los daños y perjuicios sufridos por una persona, con arreglo al artículo 82, apartados 1 y 2, de dicho Reglamento, 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», a los efectos del artículo 4, punto 10, del mencionado Reglamento.

66 Con carácter preliminar, se debe precisar que del artículo 4, punto 10, del RGPD se desprende que tienen la condición de «terceros», en particular, las personas distintas de aquellas autorizadas para tratar datos personales bajo la autoridad directa del responsable o del encargado del tratamiento. Esta definición abarca a personas que no son empleados del responsable del tratamiento y no están sujetas a su control, como las mencionadas en la cuestión planteada.

67 A continuación, procede recordar, en primer lugar, que el artículo 82, apartado 2, del 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 [este] Reglamento» y, en segundo lugar, que el apartado 3 del mismo artículo 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».

68 Por otro lado, el considerando 146 del RGPD, que se refiere específicamente al artículo 82 del mismo Reglamento, enuncia, en sus frases primera y segunda, que «el responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción de [dicho] Reglamento» y «[debe] quedar [exento] de responsabilidad si se demuestra que en modo alguno [es responsable] de los daños y perjuicios».

69 De estas disposiciones se desprende, por un lado, que el responsable del tratamiento debe, en principio, indemnizar los daños y perjuicios causados por una infracción del citado Reglamento relacionada con ese tratamiento y, por otro lado, que solo puede quedar exonerado de responsabilidad si aporta la prueba de que en modo alguno es responsable de esos daños y perjuicios.

70 Así pues, como pone de manifiesto la inclusión de la expresión «en modo alguno» durante el procedimiento legislativo, las circunstancias en las que el responsable del tratamiento puede pretender que se le exonere de la responsabilidad civil configurada por el artículo 82 del RGPD deben limitarse estrictamente a aquellas en las que dicho responsable pueda demostrar que el daño no le es imputable.

71 Cuando, como en el presente asunto, la violación de la seguridad de los datos personales, en el sentido del artículo 4, punto 12, del RGPD, ha sido cometida por cibercriminales y, por tanto, por «terceros», en el sentido del artículo 4, punto 10, de este, 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, apartado 1, letra f), 24 y 32 del mismo Reglamento.

72 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, apartado 3, del 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.

73 En segundo lugar, la interpretación anterior del referido artículo 82, apartado 3, también es conforme con el objetivo del RGPD consistente en garantizar un nivel elevado de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, enunciado en los considerandos 10 y 11 de este Reglamento.

74 Habida cuenta de todas las consideraciones anteriores, procede responder a la cuarta cuestión prejudicial que el artículo 82, apartado 3, del 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 al artículo 82, apartados 1 y 2, de dicho Reglamento, 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», a los efectos del artículo 4, punto 10, del mencionado Reglamento, pues ese responsable debe demostrar que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios en cuestión.

Quinta cuestión prejudicial

75 Mediante su quinta cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si el artículo 82, apartado 1, del 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 citado Reglamento puede constituir, por sí solo, un «daño o perjuicio inmaterial» a los efectos de la mencionada disposición.

76 En lo que se refiere, en primer lugar, al tenor del artículo 82, apartado 1, del RGPD, procede observar que este establece que «toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos».

77 A este respecto, el Tribunal de Justicia ha señalado que del tenor del artículo 82, apartado 1, del RGPD se desprende claramente que la existencia de «daños» o de «perjuicios» que se han «sufrido» constituye uno de los requisitos del derecho a indemnización previsto en dicha disposición, al igual que la existencia de una infracción del mencionado Reglamento y de una relación de causalidad entre dichos daños y perjuicios y esa infracción, de modo que estos tres requisitos son acumulativos [sentencia de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370, apartado 32].

78 Por otra parte, basándose en consideraciones de orden tanto literal como sistemático y teleológico, el Tribunal de Justicia ha interpretado el artículo 82, apartado 1, del RGPD en el sentido de que se opone a una norma o práctica nacional que supedita la indemnización por «daños y perjuicios inmateriales», en el sentido de esta disposición, al requisito de que los daños y perjuicios sufridos por el interesado hayan alcanzado cierto grado de gravedad [sentencia de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370, apartado 51].

79 Una vez recordado lo anterior, es importante subrayar, en el presente asunto, que el artículo 82, apartado 1, del RGPD no distingue entre los supuestos en los que, tras una infracción acreditada de las disposiciones de este Reglamento, 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.

80 Por consiguiente, el tenor del artículo 82, apartado 1, del RGPD no excluye que el concepto de «daños y perjuicios inmateriales» que figura en esta disposición incluya una situación, como la examinada por el órgano jurisdiccional remitente, en la que el interesado invoca, con el fin de obtener una indemnización sobre la base de la citada disposición, 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 de dicho Reglamento.

81 Esta interpretación literal se ve corroborada, en segundo lugar, por el considerando 146 del RGPD, que versa específicamente sobre el derecho a indemnización previsto en el artículo 82, apartado 1, de este Reglamento, y que se refiere, en su tercera frase, a que «el concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal

modo que se respeten plenamente los objetivos» de dicho Reglamento. Pues bien, una interpretación del concepto de «daños y perjuicios inmateriales», en el sentido del artículo 82, apartado 1, que no incluya las situaciones en las que la persona afectada por una infracción del mencionado Reglamento invoca el temor que experimenta a que sus datos personales puedan ser objeto de un uso indebido en el futuro no sería conforme con una acepción amplia del referido concepto, tal como pretende el legislador de la Unión [véase, por analogía, la sentencia de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370, apartados 37 y 46].

82 Por otra parte, el considerando 85, primera frase, del RGPD indica que «si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, […] o cualquier otro perjuicio económico o social significativo». De esta lista ilustrativa de los «daños» o los «perjuicios» que pueden sufrir los interesados se desprende que el legislador de la Unión quiso incluir en estos conceptos, en particular, la mera «pérdida de control» sobre sus datos a raíz de una infracción de aquel Reglamento, aun cuando no se haya producido un uso indebido de los datos en cuestión en perjuicio de dichas personas.

83 En tercer y último lugar, la interpretación que figura en el apartado 80 de la presente sentencia se ve corroborada por los objetivos del RGPD, que deben respetarse plenamente para definir el concepto de «daños y perjuicios», como señala el considerando 146, tercera frase, de este Reglamento. Pues bien, una interpretación del artículo 82, apartado 1, del RGPD según la cual el concepto de «daños y perjuicios inmateriales», en el sentido de esta disposición, no incluya las situaciones en las que un interesado invoca únicamente su temor a que sus datos sean objeto de un uso indebido por parte de terceros en el futuro no sería conforme con la necesidad de garantizar un elevado nivel de protección de las personas físicas en cuanto al tratamiento de datos personales en la Unión que persigue el mencionado Reglamento.

84 No obstante, es importante subrayar 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 de dicho Reglamento [sentencia de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370, apartado 50].

85 En particular, cuando una persona que solicita una indemnización por este motivo invoca el temor de que en el futuro se produzca un uso indebido de sus datos personales como consecuencia de dicha infracción, el órgano jurisdiccional que conozca del asunto deberá comprobar que ese temor puede considerarse fundado, habida cuenta de las circunstancias específicas del caso y del interesado.

86 A la luz de las consideraciones anteriores, procede responder a la quinta cuestión prejudicial que el artículo 82, apartado 1, del 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 citado Reglamento puede constituir, por sí solo, un «daño o perjuicio inmaterial» a los efectos de la mencionada disposición.

Costas

87 Dado que el procedimiento tiene, para las partes del litigio principal, el carácter de un incidente promovido ante el órgano jurisdiccional remitente, corresponde a este resolver sobre las costas. Los gastos efectuados por quienes, no siendo partes del litigio principal, han presentado observaciones ante el Tribunal de Justicia no pueden ser objeto de reembolso.

En virtud de todo lo expuesto, el Tribunal de Justicia (Sala Tercera) declara:

1) **Los artículos 24 y 32, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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 (Reglamento general de protección de datos),**

   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», a los efectos del artículo 4, punto 10, del mencionado Reglamento, no bastan, por sí solos, para considerar que las medidas técnicas y organizativas adoptadas por el responsable del tratamiento de que se trate no eran «apropiadas» con arreglo a los citados artículos 24 y 32.

2) **El artículo 32 del Reglamento 2016/679**

   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.

3) **El principio de responsabilidad del responsable del tratamiento, enunciado en el artículo 5, apartado 2, del Reglamento 2016/679 y desarrollado en el artículo 24 de este Reglamento,**

   debe interpretarse en el sentido de que,

   en el marco de una acción de indemnización basada en el artículo 82 del citado Reglamento, 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 del mencionado Reglamento.

4) **El artículo 32 del Reglamento 2016/679 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.

5) El artículo 82, apartado 3, del Reglamento 2016/679

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 al artículo 82, apartados 1 y 2, de dicho Reglamento, 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», a los efectos del artículo 4, punto 10, del mencionado Reglamento, pues ese responsable debe demostrar que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios en cuestión.

6) El artículo 82, apartado 1, del Reglamento 2016/679

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 citado Reglamento puede constituir, por sí solo, un «daño o perjuicio inmaterial» a los efectos de la mencionada disposición.

Firmas