Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
SR. GIOVANNI PITRUZZELLA
presentadas el 27 de abril de 2023 [1]

Asunto C-340/21

VB
contra
Natsionalna agentsia za prihodite

[Petición de decisión prejudicial planteada por el Varhoven administrativen sad (Tribunal Supremo de lo Contencioso-Administrativo, Bulgaria)]

«Procedimiento prejudicial — Protección de datos personales — Reglamento (UE) 2016/679 — Responsabilidad del responsable del tratamiento — Seguridad del tratamiento — Violación de la seguridad del tratamiento de los datos personales — Daño moral sufrido a causa de la inactividad del responsable del tratamiento — Acción indemnizatoria»

¿Puede la difusión ilícita de datos personales en poder de un organismo público como consecuencia de un ciberataque dar lugar a la indemnización del daño moral a favor del titular de esos datos por el mero hecho de que este tema un eventual futuro uso indebido de sus datos? ¿Cuáles son los criterios para la imputación de la responsabilidad al responsable del tratamiento? ¿Cómo se reparte la carga de la prueba en el marco del procedimiento judicial? ¿Cuál es la amplitud del control del juez?

I. Marco jurídico

1. El artículo 4, titulado «Definiciones», del Reglamento (UE) 2016/679 [2] (en lo sucesivo, «Reglamento») dispone:

«A efectos del presente Reglamento se entenderá por:

[…]

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;

[1] Lengua original: italiano.

[2] Reglamento 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).

[…]».

2. El artículo 5, bajo el epígrafe «Principios relativos al tratamiento», establece:

«1. Los datos personales serán:

[…]

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”).»

3. El artículo 24 del citado Reglamento, bajo la rúbrica, «Responsabilidad del responsable del tratamiento», establece:

«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».

4. De conformidad con el artículo 32, titulado «Seguridad del tratamiento»:

«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:

[…]

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.

[…]»

5. El artículo 82 de dicho Reglamento, bajo el epígrafe «Derecho a indemnización y responsabilidad», dispone:

«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.»

II. Hechos, procedimiento y cuestiones prejudiciales

6. El 15 de julio de 2019, los medios de comunicación búlgaros difundieron la noticia de que se había producido un acceso no autorizado al sistema informático de la Natsionalna agentsia za prihodite (Agencia Nacional de Recaudación, Bulgaria) (en lo sucesivo, «NAP»)[3] y se había publicado en Internet información fiscal y de la seguridad social de millones de personas, tanto nacionales como extranjeros.

7. Numerosas personas, entre ellas VB, recurrente en el procedimiento principal, demandaron judicialmente a la NAP solicitando la indemnización de los daños morales.

8. En el presente asunto, la recurrente en el procedimiento principal acudió al Administrativen sad Sofia-grad (Tribunal de lo Contencioso-Administrativo de la Ciudad de Sofía, Bulgaria) alegando que la NAP había infringido las normas nacionales e incumplido la obligación de tratar los datos personales, en su condición de responsable del tratamiento, de manera que se «garanti[zasen] niveles de seguridad adecuados» mediante la adopción de medidas técnicas y organizativas apropiadas, de conformidad con los artículos 24 y 32 del Reglamento. La recurrente adujo que había sufrido un daño moral que se había materializado en forma de preocupaciones y temores acerca de un futuro uso indebido de sus datos personales.

9. La parte recurrida subrayó, en cambio, que no había recibido ninguna solicitud de la recurrente en el procedimiento principal en la que se indicaran exactamente los datos personales afectados por el acceso. Por otra parte, después de tener conocimiento del acceso no autorizado, convocó reuniones con expertos para proteger los derechos e intereses de los ciudadanos. Según la NAP,

[3] La NAP es responsable del tratamiento en el sentido del artículo 4, apartado 7, del Reglamento. Con arreglo al Derecho nacional, es un organismo administrativo dotado de competencias específicas, dependiente del Ministro de Hacienda y que se encarga de liquidar, salvaguardar y recuperar los recursos de la Hacienda Pública y los créditos del Estado de carácter público y privado que establezca la ley. Al ejercer las facultades públicas que tiene atribuidas, dicho organismo trata datos personales.

no existía tampoco una relación de causalidad entre el ciberataque y el supuesto daño sufrido, pues la Agencia había instaurado todos los sistemas de gestión de procedimientos y de seguridad de la información, con arreglo a las normas internacionales vigentes en la materia.

10. El órgano jurisdiccional de primera instancia, el Administrativen sad Sofia-grad (Tribunal de lo Contencioso-Administrativo de la Ciudad de Sofía), desestimó la demanda por considerar que la divulgación de los datos no era imputable a la Agencia, que la carga de la prueba de la adecuación de las medidas adoptadas recaía sobre la recurrente y, por último, que no existían daños morales indemnizables.

11. Contra la sentencia dictada en primera instancia se interpuso recurso ante el Varhoven administrativen sad (Tribunal Supremo de lo Contencioso-Administrativo, Bulgaria). Entre las alegaciones formuladas, la recurrente en el litigio principal subrayó que el órgano jurisdiccional de primera instancia había incurrido en error al repartir la carga de la prueba de la falta de adopción de las medidas de seguridad. A su parecer, el daño moral tampoco debería ser objeto de la carga de la prueba, puesto que se trata de un daño moral efectivo y no meramente potencial.

12. La NAP, por su parte, recordó que había adoptado las medidas técnicas y organizativas necesarias en su condición de responsable del tratamiento y negó que existieran pruebas de un daño moral efectivo. A su juicio, la ansiedad y los temores son estados emocionales no indemnizables.

13. El órgano jurisdiccional remitente observó que los diversos procedimientos incoados por los perjudicados contra la NAP para la indemnización de los daños morales habían producido resultados diferentes.

14. En este contexto, el órgano jurisdiccional remitente suspendió el procedimiento y planteó al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Deben interpretarse los artículos 24 y 32 del Reglamento [2016/679] en el sentido de que basta una divulgación no autorizada o un acceso no autorizado a datos personales a efectos del artículo 4, punto 12, [de dicho Reglamento] por personas que no son funcionarios 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 eran apropiadas a efectos del artículo 32 del Reglamento [2016/679]?

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 en relación con el considerando 74 del Reglamento [2016/679] en el sentido de que en el procedimiento indemnizatorio con arreglo al artículo 82, apartado 1, [de dicho Reglamento] incumbe al responsable del tratamiento la carga de probar que las medidas técnicas y organizativas son apropiadas a efectos del artículo 32 [de ese mismo Reglamento]? ¿Puede considerarse que la obtención de un dictamen pericial es un medio de prueba necesario y suficiente para determinar si las medidas técnicas y organizativas adoptadas por el responsable del tratamiento fueron apropiadas en un caso como el presente, en el que el acceso y la divulgación no autorizados de datos personales se produjeron a consecuencia de un “ciberataque”?

4) ¿Debe interpretarse el artículo 82, apartado 3, del Reglamento [2016/679] en el sentido de que la divulgación o el acceso no autorizados a datos personales a efectos del artículo 4, punto 12, del Reglamento [2016/679], 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 exención de responsabilidad?

5) ¿Debe interpretarse el artículo 82, apartados 1 y 2, en relación con los considerandos 85 y 146 del Reglamento [2016/679] 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?»

III. Análisis jurídico

A. Observaciones preliminares

15. El presente asunto tiene por objeto cuestiones interesantes y en parte inéditas relativas a la interpretación de varias disposiciones del Reglamento. [4]

16. Las cinco cuestiones prejudiciales giran en torno al mismo tema: los requisitos para que sea indemnizable el daño moral sufrido por una persona cuyos datos personales, en poder de un organismo público, han sido publicados en Internet a raíz de un ciberataque.

17. A fin de simplificar la exposición, propondré respuestas sucintas separadas para todas las cuestiones prejudiciales planteadas en la resolución de remisión, aun sabiendo que existe un cierto solapamiento conceptual, puesto que las cuatro primeras cuestiones tienen por objeto determinar los requisitos para que la infracción de las disposiciones del Reglamento sea imputable al responsable del tratamiento [5] y la quinta se refiere, más específicamente, al concepto de daño moral a efectos de la indemnización. [6]

[4] El artículo 5, apartado 2 (relativo al principio de responsabilidad de cualquier responsable del tratamiento de datos personales), el artículo 24 (relativo a las medidas que el responsable del tratamiento está obligado a aplicar a fin de garantizar que el tratamiento es conforme al referido Reglamento), el artículo 32 (relativo a esta obligación específicamente en relación con la seguridad del tratamiento), el artículo 82, apartados 1 a 3 (relativo a la indemnización de los daños resultantes de una infracción de dicho Reglamento y a la posibilidad de que el responsable del tratamiento adopte medidas para garantizar el cumplimiento del Reglamento), y los considerandos 74, 85 y 146, que están relacionados con dichos artículos.

[5] a) En la primera cuestión se solicita que se dilucide si de la mera violación de los sistemas puede deducirse la inadecuación de las medidas establecidas; b) la segunda se refiere al alcance del control judicial de la adecuación de dichas medidas; c) la tercera tiene por objeto la carga de la prueba de dicha adecuación y ciertas modalidades técnicas para la búsqueda de la prueba; d) la cuarta versa sobre la pertinencia, a efectos de exención de la responsabilidad, de la circunstancia de que el ataque al sistema proceda del exterior.

[6] En cuanto a las disposiciones citadas del Reglamento, las tres primeras cuestiones prejudiciales versan sobre los aspectos de la responsabilidad del responsable del tratamiento relativos a la adecuación de las medidas que han de adoptarse (artículos 5, 24 y 32), y la cuarta y la quinta se refieren a los requisitos de exención de responsabilidad y al concepto de daño moral indemnizable (artículo 82).

18. Cabe señalar que actualmente están pendientes ante el Tribunal de Justicia varios asuntos relativos al artículo 82 del Reglamento y que, en uno de ellos, ya se ha dado lectura a las conclusiones del Abogado General, que tendré en cuenta en el presente análisis. [7]

19. Antes de examinar las cuestiones planteadas, estimo oportuno exponer algunas observaciones preliminares acerca de los principios y la finalidad del Reglamento, que resultarán útiles para responder a cada una de las cuestiones prejudiciales.

20. El artículo 24 del Reglamento establece en términos generales la obligación del responsable del tratamiento de aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de los datos personales es conforme con dicho Reglamento, mientras que el artículo 32 prevé más específicamente esa misma obligación en lo que se refiere a la seguridad del tratamiento. Los artículos 24 y 32 desarrollan de forma más específica lo ya previsto en el artículo 5, apartado 2, que introduce, precisamente entre los «principios relativos al tratamiento», el «principio de responsabilidad proactiva». Este principio se deriva lógicamente y es complementario del «principio de integridad y confidencialidad» enunciado en el artículo 5, apartado 1, letra f), y ambos principios deben interpretarse a la luz del enfoque basado en el riesgo en que se fundamenta el Reglamento.

21. El principio de responsabilidad proactiva es uno de los pilares del Reglamento y una de sus innovaciones más significativas. Atribuye al responsable del tratamiento la responsabilidad de adoptar medidas proactivas a fin de garantizar y poder demostrar la conformidad con el Reglamento. [8]

22. La doctrina ha hablado de un auténtico cambio cultural como consecuencia del «alcance global de la obligación de responsabilidad». [9] No es tanto el cumplimiento formal de la obligación legal o de una medida puntual, sino toda la estrategia empresarial adoptada lo que exime de responsabilidad al responsable del tratamiento por ser *conforme* con la normativa de protección de datos.

23. Las medidas técnicas y organizativas que requiere el principio de responsabilidad proactiva deben ser «apropiadas» teniendo en cuenta los factores especificados en el artículo 24: la naturaleza, el ámbito, el contexto y la finalidad del tratamiento, así como la probabilidad y gravedad de los riesgos para los derechos y libertades de las personas físicas.

24. El artículo 24 exige, por tanto, que las medidas sean apropiadas a fin de poder demostrar que el tratamiento es conforme con los principios y las disposiciones del Reglamento.

25. El artículo 32, en cambio, proyecta el principio de responsabilidad proactiva sobre las medidas concretas que han de adoptarse a fin de garantizar «un nivel de seguridad adecuado al riesgo». Para ello, a los factores ya previstos que deben tenerse en cuenta en la elaboración de las medidas técnicas y organizativas, añade el estado de la técnica y los costes de aplicación.

[7] Véanse las conclusiones del Abogado General Campos Sánchez-Bordona presentadas en el asunto Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales) (C-300/21, EU:C:2022:756).

[8] Docksey, C.: «Article 24. Responsibility of the controller», Kuner, C., Bygrave, L. A., Docksey, C. y Drechsler, L.: *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 561. Los principios y las obligaciones de las normas sobre protección de datos deben inspirar el tejido cultural de las organizaciones, a todos los niveles, en lugar de considerarse como una serie de requisitos legales que han de ser comprobados por el departamento jurídico.

[9] Belisario, E., Riccio, G. y Scorza, G.: *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 301.

26. El concepto de adecuación requiere que las soluciones adoptadas para garantizar los sistemas informáticos alcancen un nivel aceptable, tanto en términos técnicos (pertinencia de las medidas) como cualitativos (eficacia de la protección). Para garantizar el cumplimiento de los principios de necesidad, pertinencia y proporcionalidad, los tratamientos deben ser no solo idóneos, sino también satisfactorios en lo que respecta a las finalidades que se pretenden alcanzar. En este sentido, juega un papel decisivo el principio de minimización, en virtud del cual las fases del tratamiento de datos deben perseguir constantemente reducir al mínimo los riesgos de seguridad. [10]

27. Todo el Reglamento se basa en la prevención del riesgo y la responsabilidad proactiva del responsable del tratamiento y, por tanto, en un enfoque teleológico que persigue el mejor resultado posible en términos de eficacia, es decir, muy lejos de la lógica formalista vinculada a la mera obligación de cumplir procedimientos específicos que eximan de responsabilidad. [11]

28. El artículo 24 no contiene una enumeración exhaustiva de las medidas «apropiadas»: deberá realizarse una valoración caso por caso. Ello está en consonancia con la filosofía del Reglamento, según la cual es preferible que los procedimientos que se adopten se elijan a la luz de una valoración cuidadosa de la situación específica de modo que puedan ser lo más eficaces posible. [12]

B. Primera cuestión prejudicial

29. Mediante su primera cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si los artículos 24 y 32 del Reglamento deben interpretarse en el sentido de que el hecho de que se haya producido una «violación de la seguridad de los datos personales», tal como se define en el artículo 4, apartado 12, basta por sí solo para concluir que las medidas técnicas y organizativas aplicadas por el responsable del tratamiento no eran «apropiadas» para garantizar la protección de los datos.

30. Del tenor de los artículos 24 y 32 del Reglamento se desprende que el responsable del tratamiento, al elegir las medidas técnicas y organizativas que está obligado a aplicar para garantizar la conformidad con dicho Reglamento, debe tener en cuenta una serie de factores de valoración que se enumeran en tales artículos y que se han mencionado anteriormente.

31. El responsable del tratamiento dispone de cierto margen de apreciación para determinar las medidas más apropiadas a la luz de su situación específica, pero esta elección está sujeta en todo caso a un eventual control jurisdiccional de la conformidad de las medidas aplicadas con todas las obligaciones y las finalidades del referido Reglamento.

[10] Belisario, E., Riccio, G. y Scorza, G., *op. cit.*, p. 380.

[11] Por ello, como se explicará, las cuestiones prejudiciales primera y cuarta no pueden responderse más que en sentido negativo. De las disposiciones del Reglamento no puede deducirse ninguna forma de automatismo: el mero hecho de que se produzca una divulgación de datos personales no es suficiente para considerar que las medidas técnicas y organizativas adoptadas no son apropiadas, ni tampoco la circunstancia de que la divulgación haya tenido lugar por la intervención de personas ajenas a la organización del responsable del tratamiento y no sujetas al ámbito de control de este basta para eximirlo de responsabilidad.

[12] Bolognini, L. y Pelino, E.: *Codice della disciplina privacy*, Giuffrè, 2019, p. 201. El legislador europeo supera, por tanto, la concepción de la seguridad del tratamiento basada en la existencia de medidas de seguridad predeterminadas y adopta la metodología propia de las normas internacionales en materia de gestión de sistemas de información basada en el riesgo: prevé la determinación de medidas de mitigación de los riesgos que prescinden de *checklists* (listas de control) preconfiguradas y que son aplicables de modo genérico. Por consiguiente, es necesario acudir a las directrices y normas internacionales. El resultado de esta valoración de los riesgos adquiere carácter vinculante en el momento en que la organización toma decisiones para mitigar los riesgos identificados, haciéndose *accountable* (responsable).

32. En particular, por lo que respecta a las medidas de seguridad, el artículo 32, apartado 1, exige al responsable del tratamiento que tenga en cuenta el «estado de la técnica». Ello implica una limitación del nivel tecnológico de las medidas que han de aplicarse a lo que sea razonablemente posible en el momento de la adopción de dichas medidas: la idoneidad de la medida para prevenir el riesgo debe ser proporcionada a las soluciones que ofrece el estado de desarrollo de la ciencia, la técnica, la tecnología y la investigación existentes, tomando también en consideración, como se verá, los costes de aplicación.

33. Las medidas pueden ser «apropiadas» en un momento determinado y, no obstante, ser burladas por ciberdelincuentes que utilizan instrumentos muy sofisticados que permitan vulnerar incluso las medidas de seguridad que son conformes con el estado de la técnica.

34. Por otra parte, no parece lógico considerar que el legislador de la Unión tuviera intención de imponer al responsable del tratamiento la obligación de prevenir cualquier violación de la seguridad de los datos personales, con independencia de la diligencia aplicada en la elaboración de las medidas de seguridad. [13]

35. Como se ha indicado antes, el Reglamento se aleja de todo automatismo, exigiendo una elevada responsabilidad proactiva del responsable del tratamiento, lo cual, sin embargo, no puede conducir a que resulte imposible para este último demostrar que ha cumplido correctamente las obligaciones que le incumben.

36. Además, con arreglo al artículo 32, apartado 1, han de tenerse en cuenta, tal como se ha señalado, los «costes de aplicación» de las medidas técnicas y organizativas de que se trate. De ello se deduce que la valoración de la adecuación de dichas medidas debe basarse en una ponderación entre los intereses de la persona afectada, que en general postulan un nivel de protección más alto, y los intereses económicos y la capacidad tecnológica del responsable del tratamiento, que en ocasiones propician un nivel de protección inferior. Dicha ponderación ha de respetar los requisitos del principio general de proporcionalidad.

37. A ello debe añadirse, desde el punto de vista de la interpretación sistemática, que el legislador contempla la posibilidad de que se produzcan violaciones de los sistemas; el artículo 32, apartado 1, letra c), incluye, entre las medidas propuestas, la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico. La inclusión de esta capacidad entre las medidas de seguridad que garantizan un nivel de seguridad adecuado al riesgo sería inútil si se considerase que la simple violación de los sistemas constituye en sí misma la prueba de la inadecuación de tales medidas.

C. Segunda cuestión prejudicial

38. Mediante la segunda cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, cuál debe ser el objeto y el alcance del control judicial al comprobar la adecuación de las medidas técnicas y organizativas aplicadas por el responsable del tratamiento de los datos personales con arreglo al artículo 32 del Reglamento.

[13] El concepto de adecuación denota de forma inequívoca la intención de no atribuir pertinencia a todas las medidas técnicas y organizativas teóricamente posibles. Véase, en este sentido, Gambini, M.: «Responsabilità e risarcimento nel trattamento dei dati personali», en Cuffaro, V., D'Orazio, R. y Ricciuto, V.: *I dati personali nel diritto europeo*, Giappichelli, 2019, p. 1059.

39. Ante la diversidad de situaciones que pueden presentarse en la práctica, el Reglamento no establece, como se ha dicho, disposiciones vinculantes para determinar las medidas técnicas y organizativas que el responsable del tratamiento debe adoptar para cumplir los requisitos del citado Reglamento. La adecuación de las medidas adoptadas deberá valorarse, pues, en el caso concreto, comprobando si las medidas concretas son idóneas para prevenir razonablemente el riesgo y reducir al mínimo los efectos negativos de la infracción.

40. Si bien es indudablemente cierto que la elección y aplicación de dichas medidas forma parte de la valoración subjetiva del responsable del tratamiento, puesto que las medidas mencionadas en el Reglamento solo son ejemplos, el examen del juez no puede limitarse a controlar si el responsable del tratamiento ha cumplido las obligaciones derivadas de los artículos 24 y 32, es decir, si ha previsto (formalmente) determinadas medidas técnicas y organizativas. Debe realizar un análisis concreto del contenido de tales medidas, del modo en que se aplican y de sus efectos prácticos, sobre la base de los elementos de prueba de los que dispone y de las circunstancias del caso específico. Como ha observado acertadamente el Gobierno portugués, «el modo de cumplimiento de sus obligaciones resulta inseparable del contenido de las medidas adoptadas a efectos de demostrar que, teniendo en cuenta el tratamiento específico de los datos (su naturaleza, alcance, contexto y finalidad), el estado actual de las tecnologías disponibles y sus costes, así como los riesgos para los derechos y libertades de los ciudadanos, el responsable del tratamiento ha adoptado todas las medidas necesarias y apropiadas para garantizar un nivel de seguridad adecuado al riesgo subyacente». [14]

41. Por consiguiente, el control judicial deberá tener en cuenta todos los factores mencionados en los artículos 24 y 32 que, como se ha indicado, enumeran una serie de criterios para valorar la adecuación y ofrecen ejemplos de medidas que pueden considerarse adecuadas. Asimismo, como subrayaron la Comisión Europea y todos los Estados miembros que presentaron observaciones sobre la segunda cuestión prejudicial, el artículo 32, apartados 1 a 3, pone de relieve la necesidad de «garantizar un nivel de seguridad adecuado al riesgo», indicando otros factores pertinentes al efecto, como la eventual adopción por el responsable del tratamiento de un código de conducta aprobado o de un mecanismo de certificación aprobado, tal como prevén respectivamente los artículos 40 y 42 del Reglamento.

42. La adopción de códigos de conducta o mecanismos de certificación puede ofrecer un elemento útil de valoración a efectos de la satisfacción de la carga de la prueba y del consiguiente control judicial. Sin embargo, ha de precisarse que no basta que el responsable del tratamiento se adhiera a un código de conducta, sino que tiene la carga de demostrar que ha adoptado en concreto las medidas que prevé dicho código, de conformidad con el principio de responsabilidad proactiva. La certificación, en cambio, constituye «por sí misma una demostración de que los tratamientos de datos realizados son conformes con el Reglamento, aunque puede ser refutada en la práctica». [15]

[14] Observaciones escritas, apartado 31.

[15] Gambini, M., *op. cit.*, p. 1067. La posesión de una certificación genera, por tanto, una inversión de la carga de la prueba en favor del responsable del tratamiento, a quien se facilita la demostración de que ha actuado respetando las obligaciones establecidas en el Reglamento.

43. Por último, procede observar que, en virtud del artículo 24, apartado 1, esas medidas deben revisarse y actualizarse cuando sea necesario. Y también esto será objeto de la apreciación del juez nacional. El artículo 32, apartado 1, del Reglamento [16] impone, en efecto, al responsable del tratamiento una carga de control y supervisión constante, preventiva y subsiguiente respecto a las actividades de tratamiento, pero también de mantenimiento y posible actualización de las medidas adoptadas, con el fin tanto de prevenir las violaciones como de limitar, en su caso, sus efectos.

44. Sin embargo, me inclino por descartar la posibilidad de que la sentencia que ha de dictarse incluya una lista de elementos sustanciales, como la propuesta por el Gobierno portugués. [17] Ello podría dar lugar a interpretaciones contradictorias, ya que obviamente la lista nunca puede ser exhaustiva.

D. Tercera cuestión prejudicial

45. Mediante la primera parte de la tercera cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia si, habida cuenta del principio de responsabilidad proactiva de los artículos 5, apartado 2, y 24, en relación con el considerando 74 [18] del Reglamento, en el marco de una demanda de indemnización de daños en virtud del artículo 82, la carga de la prueba de la adecuación de las medidas técnicas y organizativas con arreglo al artículo 32 recae sobre el responsable del tratamiento de los datos personales.

46. Las consideraciones antes expuestas me permiten responder de modo conciso a esta cuestión en sentido afirmativo.

47. En efecto, la letra, el contexto y la finalidad del Reglamento abogan de forma unívoca a favor de que la carga de la prueba recaiga sobre el responsable del tratamiento.

48. De la formulación de varias disposiciones del Reglamento se desprende que el responsable del tratamiento ha de «poder» o ser «capaz» de «demostrar» el cumplimiento de las obligaciones establecidas en el Reglamento y, en particular, que ha aplicado medidas apropiadas a este efecto, tal como se indica en el considerando 74 y en los artículos 5, apartado 2, y 24, apartado 1. Como

[16] Al disponer expresamente, en la letra d), que la apreciación de la adecuación comprende la eficacia de las medidas adoptadas, que debe ser verificada, evaluada y valorada regularmente, tanto en la fase inicial como con carácter periódico, con el fin de garantizar la seguridad efectiva de todos los tipos de tratamiento, cualquiera que sea su nivel de riesgo, y, además, al prever de modo expreso, en la letra c), que las medidas técnicas y organizativas aplicadas deben tener la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico. Véase Gambini, M., *op. cit.*, pp. 1064 y 1065.

[17] Apartado 30 de las observaciones escritas: «Corresponderá al responsable del tratamiento demostrar cómo ha valorado todos los factores y circunstancias relativos al tratamiento en cuestión y, en particular, el resultado del análisis realizado de los riesgos, los riesgos identificados, las medidas concretas tomadas para mitigar dichos riesgos, la justificación de las opciones elegidas a la luz de las soluciones tecnológicas disponibles en el mercado, la eficacia de las medidas, la correlación entre las medidas técnicas y organizativas, la formación del personal que realiza el tratamiento de los datos, la existencia de una externalización de las operaciones de tratamiento de datos, incluido el desarrollo y mantenimiento de las tecnologías informáticas, y la existencia de un control por parte del responsable del tratamiento y de instrucciones precisas impartidas a los encargados del tratamiento, en el sentido del artículo 28 del Reglamento General de Protección de Datos, relativas al tratamiento de datos personales por parte de estos últimos; cómo se ha valorado la infraestructura de soporte de los sistemas de comunicación e información y cómo se ha clasificado el nivel de riesgo para los derechos y libertades de los interesados».

[18] A tenor del considerando 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».

subraya el Gobierno portugués, el citado considerando 74 especifica que la carga de la prueba así impuesta al responsable debe comprender la demostración de la «eficacia de las medidas» en cuestión.

49. En mi opinión, esta interpretación literal se ve corroborada por las siguientes consideraciones prácticas y teleológicas.

50. En lo que atañe al reparto de la carga de la prueba, en una demanda de indemnización de daños basada en el artículo 82, el interesado que ha presentado la demanda contra el responsable del tratamiento debe demostrar, en primer lugar, que se ha producido una infracción del Reglamento, en segundo lugar, que ha sufrido un daño y, en tercer lugar, que existe una relación de causalidad entre estos dos elementos, tal como se ha señalado en todas las observaciones escritas relativas a la quinta cuestión prejudicial. Se trata de tres requisitos acumulativos, según se desprende también de reiterada jurisprudencia del Tribunal de Justicia y del Tribunal General en el contexto de la responsabilidad extracontractual de la Unión Europea. [19]

51. Sin embargo, estimo que la obligación del demandante de demostrar la existencia de una infracción del Reglamento no puede llegar hasta el punto de exigirle acreditar que las medidas técnicas y organizativas aplicadas por el responsable del tratamiento no son apropiadas en el sentido de los artículos 24 y 32.

52. Como la Comisión ha destacado, la aportación de tales pruebas sería casi imposible en la práctica, ya que por lo general los interesados no tienen conocimientos suficientes para poder analizar dichas medidas ni disponen de acceso a toda la información que posee el responsable del tratamiento en cuestión, en particular en lo que respecta a los métodos aplicados para garantizar la seguridad del tratamiento. Además, el responsable del tratamiento podría alegar en ocasiones que su negativa a revelar estos hechos a los interesados se basa en el motivo legítimo de no hacer públicos sus asuntos internos o en elementos protegidos por el secreto profesional, en particular precisamente por razones de seguridad.

53. Por tanto, si se considerase que la carga de la prueba recae sobre la persona interesada, el resultado práctico consistiría en que el derecho de recurso previsto en el artículo 82, apartado 1, quedaría privado de gran parte de su contenido. A mi juicio, este resultado no está en consonancia con la intención del legislador de la Unión que, al adoptar el referido Reglamento, pretendió reforzar los derechos de los interesados y las obligaciones de los responsables del tratamiento con respecto a los establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31), a la que sustituyó. Por consiguiente, resulta lógico y jurídicamente sostenible que el responsable del tratamiento esté obligado a demostrar, al ejercer su defensa ante una demanda de indemnización de daños, que ha cumplido todas las obligaciones dimanantes de los artículos 24 y 32 de dicho Reglamento adoptando medidas efectivamente apropiadas.

[19] Véanse, en particular, las sentencias del Tribunal de Justicia de 5 de septiembre de 2019, Unión Europea/Guardian Europe y Guardian Europe/Unión Europea (C-447/17 P y C-479/17 P, EU:C:2019:672), apartado 147, y de 28 de octubre de 2021, Vialto Consulting/Comisión (C-650/19 P, EU:C:2021:879), apartado 138, así como las sentencias del Tribunal General de 13 de enero de 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4), apartado 116, y de 29 de septiembre de 2021, Kočner/Europol (T-528/20, no publicada, EU:T:2021:631), apartado 61, en la que se recuerda que deben concurrir tres requisitos, a saber, «la ilicitud de la actuación imputada a la institución de la Unión, la realidad del daño y la existencia de una relación de causalidad entre la actuación de dicha institución y el perjuicio invocado».

54. Mediante la segunda parte de la tercera cuestión prejudicial, el órgano jurisdiccional remitente pregunta al Tribunal de Justicia, en esencia, si un dictamen judicial puede considerarse un medio de prueba necesario y suficiente para valorar la adecuación de las medidas técnicas y organizativas aplicadas por el responsable del tratamiento de los datos personales en una situación en la que el acceso y la divulgación no autorizados de los datos personales se produjeron a consecuencia de un ciberataque.

55. Considero, como han subrayado, en esencia, los Gobiernos búlgaro e italiano, Irlanda y la Comisión, que la respuesta a esta cuestión debe basarse en la reiterada jurisprudencia del Tribunal de Justicia conforme a la cual, en virtud del principio de autonomía procesal, a falta de normas de la Unión en la materia, corresponde al ordenamiento jurídico interno de cada Estado miembro regular las modalidades procesales de los procedimientos judiciales destinados a proteger los derechos de las personas, siempre y cuando, no obstante, esas normas no sean, en las situaciones reguladas por el Derecho de la Unión, menos favorables que las que rigen situaciones similares sometidas al Derecho nacional (principio de equivalencia) y no hagan imposible en la práctica o excesivamente difícil el ejercicio de los derechos conferidos por el Derecho de la Unión (principio de efectividad).

56. En el presente asunto, debo observar que el Reglamento no contiene ninguna disposición dirigida a determinar los medios de prueba admisibles y su valor probatorio, en particular en relación con las diligencias de prueba (como el dictamen pericial) que los tribunales nacionales pueden o deben ordenar para dilucidar si el responsable del tratamiento de los datos personales ha adoptado medidas apropiadas en el sentido del Reglamento. En consecuencia, estimo que, a falta de normas armonizadas en la materia, corresponde al ordenamiento jurídico interno de cada Estado miembro determinar esas modalidades procesales, siempre que se respeten los principios de equivalencia y de efectividad.

57. El citado «principio de efectividad», que implica que un juez independiente debe realizar una valoración imparcial, podría verse comprometido si el adjetivo «suficiente» se entendiera en el sentido que, según mi entender, le atribuye el órgano jurisdiccional remitente, es decir, en el sentido de que puede deducirse automáticamente de un dictamen pericial que las medidas adoptadas por el responsable del tratamiento son apropiadas. [20]

E. Cuarta cuestión prejudicial

58. Mediante la cuarta cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si el artículo 82, apartado 3, del Reglamento debe interpretarse en el sentido de que una infracción de dicho Reglamento (consistente, como en el presente asunto, en la «comunicación o acceso no autorizados» a los datos personales en el sentido del artículo 4, apartado 12) por parte de personas que no son empleados del responsable del tratamiento de tales datos y que no están sometidas al control de este constituye un hecho no imputable en modo alguno al responsable del tratamiento y, por tanto, un motivo de exención de su responsabilidad con arreglo al artículo 82, apartado 3.

[20] Observaciones escritas, apartado 39.

59. La respuesta a esta cuestión se desprende de manera directa de las consideraciones antes expuestas acerca de la filosofía general del Reglamento: no se prevén automatismos y, en consecuencia, el mero hecho de que la comunicación de los datos personales o el acceso no autorizado a los mismos se haya producido a causa de personas no sujetas al ámbito de control del responsable del tratamiento no exime de responsabilidad a este último.

60. En primer lugar, en términos literales, debe señalarse que ni el artículo 82, apartado 3, ni el considerando 146 indican requisitos particulares que el responsable del tratamiento pueda cumplir para quedar exento de responsabilidad, salvo la demostración de que «no es en modo alguno responsable del hecho que haya causado los daños y perjuicios». De esta formulación se desprende, por una parte, que el responsable del tratamiento solo puede ser exonerado de responsabilidad si demuestra que el hecho causante del daño de que se trate no le es imputable y, por otra parte, que el nivel de prueba requerido por esta disposición es elevado, teniendo en cuenta el uso de la expresión «en modo alguno», tal como ha recalcado la Comisión. [21]

61. El régimen de responsabilidad previsto en el artículo 82 y, más en general, en el Reglamento en su conjunto ha sido objeto de amplio debate en la doctrina de diversos Estados miembros. Contiene, en efecto, elementos tradicionales propios de la responsabilidad extracontractual, pero también elementos que, por la estructura de las disposiciones, lo aproximan a la responsabilidad contractual o incluso a una modalidad de responsabilidad objetiva, en razón de la peligrosidad intrínseca de la actividad de tratamiento de datos. No es esta la ocasión para exponer el debate que se ha desarrollado, pero, en mi opinión, no estimo que el artículo 82 establezca un régimen de responsabilidad objetiva. [22]

62. El daño resultante de la violación de la seguridad de los datos personales puede producirse como consecuencia culposa de la falta de adopción de las medidas técnicas y organizativas razonables y, en cualquier caso, apropiadas para prevenirlo, teniendo en cuenta los riesgos para los derechos y libertades de las personas que resultan de la actividad de tratamiento. Dichos riesgos hacen más rigurosa la obligación de prevenir y evitar el daño, ampliando el deber de diligencia que incumbe al responsable del tratamiento. Por consiguiente, de la lectura combinada de las obligaciones de conducta que incumben a los responsables del tratamiento y de la disposición sobre la prueba de descargo en lo que concierne al causante del daño, es posible inferir argumentos a favor de reconocer la naturaleza de responsabilidad agravada por culpa presunta al supuesto de responsabilidad por tratamiento ilícito de datos personales previsto en el artículo 82 del Reglamento. [23]

63. De ello se desprende la posibilidad de que el responsable del tratamiento presente una prueba de descargo (que no se permite en el caso de la responsabilidad objetiva). En lo que atañe a la articulación de la carga probatoria, el artículo 82, apartado 3, del Reglamento prevé un régimen

[21] De conformidad con la reiterada jurisprudencia del Tribunal de Justicia según la cual las excepciones a una norma general deben interpretarse de forma restrictiva, la eventual exención de responsabilidad prevista en el artículo 82, apartado 3, ha de interpretarse restrictivamente. Véanse, por analogía, las sentencias de 15 de octubre de 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831), apartado 53, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros (C-140/20, EU:C:2022:258), apartado 40.

[22] La responsabilidad civil tiende a calificarse de objetiva cuando el agente esté obligado a adoptar todas las medidas teóricamente posibles para evitar el daño, al margen del conocimiento efectivo que tenga al respecto o de su sostenibilidad económica. Por el contrario, cuando se exija al agente adoptar las medidas normalmente aplicables por un operador del sector económico de referencia para mantener la seguridad y prevenir los perjuicios que puedan derivarse de la actividad ejercida, la imputación del daño tiende a desplazarse hacia un régimen de responsabilidad por culpa específica. Gambini, M., *op. cit.*, p. 1055.

[23] Gambini, M., *op. cit.*, p. 1059. En sentido análogo, en lo que respecta a la tesis según la cual la prueba de la adopción de las medidas idóneas consiste no solo en alegar simplemente la máxima diligencia exigible, sino en demostrar un hecho ajeno causante del daño que revista las características de imprevisibilidad e inevitabilidad propias del caso fortuito y de la fuerza mayor, véase Sica, S.: «Sub. art. 82», en D'Orazio, R., Finocchiaro, G., Pollicino, O. y Resta, G.: *Codice della privacy e data protection*, Giuffrè, 2021.

favorable al perjudicado, estableciendo un sistema de inversión de la carga de la prueba de la culpa del causante del daño,[24] en total simetría con la inversión de la carga de la prueba antes mencionada en relación con la adecuación de las medidas adoptadas. El legislador pone de manifiesto así que es consciente de los peligros que entraña establecer un reparto distinto de la carga probatoria; si se exigiera a la persona física perjudicada demostrar la culpa del causante del daño, su posición resultaría excesivamente onerosa y, por tanto, se pondría en peligro, en la práctica, la operatividad de la protección indemnizatoria en un ámbito normativo vinculado al uso de las nuevas tecnologías. En efecto, podría resultar especialmente gravoso para el interesado reconstruir y tener acceso al modo en que tuvo lugar el daño y, por consiguiente, demostrar la culpa del responsable. Por el contrario, el responsable del tratamiento se encuentra en una posición óptima para aportar la prueba de descargo que acredite que no es en modo alguno responsable del hecho que ha causado los daños.[25]

64. El responsable del tratamiento deberá demostrar también, de acuerdo con el principio de responsabilidad proactiva antes descrito, que ha hecho todo lo posible para restaurar la disponibilidad y el acceso a los datos personales de forma rápida.

65. Volviendo a la cuestión planteada por el órgano jurisdiccional remitente, sobre la base de las consideraciones antes expuestas en torno a la naturaleza de la responsabilidad del responsable del tratamiento, si bien, como se ha indicado, este puede quedar exento de responsabilidad demostrando que la infracción se debe a una causa que no le es imputable en modo alguno, no puede considerarse como tal la simple circunstancia de que el hecho haya sido causado por una persona no sujeta a su ámbito de control.

66. Cuando un responsable del tratamiento es víctima de un ataque por parte de un ciberdelincuente, puede considerarse que el hecho generador del daño no le es imputable, pero no se descarta que la negligencia del responsable del tratamiento de los datos haya estado en el origen del ataque en cuestión, facilitándolo por la falta o inadecuación de las medidas de seguridad de los datos personales que este último está obligado a aplicar. Se trata de apreciaciones de hecho específicas para cada caso, que corresponden al juez nacional que conoce del asunto, a la luz de las pruebas que se le han presentado.

67. Además, según la experiencia común, los ataques externos a los sistemas de entidades públicas o privadas titulares de un gran volumen de datos personales son mucho más frecuentes que los ataques internos. El responsable del tratamiento debe, por tanto, instaurar medidas apropiadas para hacer frente, en particular, a los ataques externos.

68. En último lugar, desde un punto de vista teleológico, debe señalarse que el Reglamento persigue el objetivo de alcanzar un nivel elevado de protección. A este respecto, el Tribunal de Justicia ya ha subrayado que se desprende del artículo 1, apartado 2, del Reglamento, en relación con sus considerandos 10, 11 y 13, que dicho Reglamento impone a las instituciones, órganos y organismos de la Unión, así como a las autoridades competentes de los Estados miembros, la misión de asegurar un nivel elevado de tutela de los derechos relativos a la protección de los datos personales garantizados por el artículo 16 TFUE y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.[26]

[24] «Si *demuestra* que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios» (artículo 82, apartado 3).

[25] Gambini, M, *op. cit.*, p. 1060.

[26] Véase, en este sentido, la sentencia de 15 de junio de 2021, Facebook Ireland y otros (C-645/19, EU:C:2021:483), apartados 44 y 45.

69. Si el Tribunal de Justicia optase por la interpretación según la cual, cuando la infracción del Reglamento ha sido cometida por un tercero, el responsable del tratamiento debe quedar automáticamente exento de responsabilidad en virtud del artículo 82, apartado 3, esta interpretación tendría un efecto incompatible con el objetivo de protección perseguido por dicho Reglamento, ya que debilitaría los derechos de los interesados, pues la responsabilidad quedaría limitada a los casos en que la infracción se deba a personas sujetas a la autoridad y/o el control del responsable del tratamiento.

F. Quinta cuestión prejudicial

70. Mediante la quinta cuestión prejudicial, el órgano jurisdiccional nacional solicita al Tribunal de Justicia, en esencia, que interprete el concepto de «daño moral» («inmaterial», en la terminología del Reglamento) en el sentido del artículo 82 del Reglamento. En particular, pregunta si las disposiciones del artículo 82, apartados 1 y 2, del Reglamento, en relación con sus considerandos 85 y146,[27] deben interpretarse en el sentido de que, en una situación en la que se cometió una infracción de dicho Reglamento consistente en el acceso no autorizado a datos personales y la difusión no autorizada de dichos datos por parte de ciberdelincuentes, el hecho de que el interesado tema un potencial futuro uso indebido de sus datos personales puede constituir en sí mismo un daño (moral) que confiere derecho a indemnización.

71. Ni el artículo 82 ni los considerandos relativos a la indemnización de los daños y perjuicios aportan una respuesta clara a esta cuestión, pero cabe inferir de ellos algunos elementos útiles para el análisis: los daños inmateriales (o morales) pueden ser objeto de indemnización además de los materiales (o patrimoniales); de la infracción del Reglamento no se deriva automáticamente el daño «causado» por esta o, más exactamente, la violación de la seguridad de los datos personales «puede entrañar» daños físicos, materiales o inmateriales para las personas físicas; el concepto de daño 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 Reglamento, y la indemnización de los daños y perjuicios «sufridos» debe ser «total y efectiva».

72. El tenor literal de las disposiciones del Reglamento descarta desde un principio cualquier posible hipótesis de daños *in re ipsa*: el objetivo principal de la responsabilidad civil que establece el Reglamento consiste en ofrecer una reparación al interesado, precisamente a través de una indemnización «total y efectiva» del daño sufrido y, por tanto, restablecer el equilibrio de la situación jurídica alterada negativamente por la infracción del Derecho.[28]

[27] A tenor del considerando 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 […]». De conformidad con el considerando 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. […]. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos […]».

[28] Véanse las conclusiones del Abogado General Campos Sánchez-Bordona presentadas en el asunto Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales) (C-300/21, EU:C:2022:756), punto 29 y nota 11. En dichas conclusiones, el Abogado General, tras llevar a cabo acertadamente su análisis desde el punto de vista literal, histórico, contextual y teleológico, excluye la naturaleza «punitiva» de los daños indemnizables a los interesados al amparo del artículo 82 (puntos 27 a 55), señalando, por un lado, que los Estados miembros «no tienen que elegir (ni pueden, en realidad) entre los mecanismos del capítulo VIII para garantizar la protección de datos. Ante una infracción que no genere daño, al interesado se le brinda aún (como mínimo) el derecho a presentar una reclamación ante una autoridad de control» y, por otro, que «la perspectiva de obtener compensación al margen de cualquier daño estimularía, probablemente, los litigios en vía civil, con demandas quizá no siempre justificadas, y, en esa medida, podría desincentivar la actividad de tratamiento de datos» (puntos 54 y 55).

73. Por otra parte, también desde el punto de vista sistemático, el Reglamento prevé, al igual que en el Derecho de defensa de la competencia, dos pilares de protección: uno de carácter público, estableciendo sanciones para las infracciones de las normas del Reglamento, y otro de carácter privado, previendo precisamente una responsabilidad civil extracontractual, que puede calificarse de agravada por culpa presunta, con las características antes señaladas, en particular con respecto a la prueba de descargo. [29]

74. Por consiguiente, una interpretación amplia [30] del concepto de daño (moral) no puede llevar a considerar que el legislador haya renunciado a la necesidad de que exista un auténtico «daño».

75. El verdadero problema de fondo consiste en si, una vez comprobada la existencia de la infracción y la relación de causalidad, puede nacer un derecho a indemnización como consecuencia de simples inquietudes, ansiedades y temores de la persona interesada acerca de un eventual futuro uso indebido de los datos personales, cuando ese uso indebido no se ha acreditado y/o la persona interesada no ha sufrido ningún otro perjuicio.

76. Según reiterada jurisprudencia del Tribunal de Justicia, los conceptos de una disposición del Derecho de la Unión que no se remita expresamente al Derecho de los Estados miembros para determinar su sentido y su alcance normalmente deben ser objeto de una interpretación autónoma y uniforme en toda la Unión, que debe buscarse teniendo en cuenta no solo el tenor literal de la disposición en cuestión, sino también el contexto en el que se inscribe, los objetivos que persigue el acto del que forma parte y la génesis de dicha disposición. [31]

77. El Tribunal de Justicia, como recordó el Abogado General Campos Sánchez-Bordona, [32] no ha elaborado una definición general de «daños y perjuicios» aplicable indistintamente en cualquier ámbito. [33] En lo que atañe a los daños morales, de su jurisprudencia puede inferirse que, cuando el objetivo (o uno de los objetivos) de la disposición que se interpreta es la protección de la persona o de cierta categoría de personas, [34] el concepto de daños y perjuicios debe ser amplio; en coherencia con ese criterio, la indemnización se extiende a los daños inmateriales, aun cuando no se mencionen en la disposición interpretada. [35]

[29] Negar el derecho a indemnización por los sentimientos o emociones débiles y pasajeros ligados a la infracción de reglas sobre el tratamiento no deja, por tanto, al interesado en completo desamparo (véanse, en este sentido, las conclusiones del Abogado General Campos Sánchez-Bordona presentadas en el asunto Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales) (C-300/21, EU:C:2022:756), punto 115).

[30] O «en sentido amplio» en los términos del considerando 146.

[31] Véanse las sentencias de 15 de abril de 2021, The North of England P & I Association (C-786/19, EU:C:2021:276), apartado 48, y de 10 de junio de 2021, KRONE — Verlag (C-65/20, EU:C:2021:471), apartado 25.

[32] Véanse las conclusiones del Abogado General Campos Sánchez-Bordona presentadas en el asunto Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales) (C-300/21, EU:C:2022:756), punto 104.

[33] No ha señalado tampoco un método de interpretación —autónoma o por remisión a los ordenamientos nacionales— como preferente: depende de la materia objeto de examen. Véanse las sentencias de 10 de mayo de 2001, Veedfald (C-203/99, EU:C:2001:258), apartado 27, en materia de productos defectuosos; de 6 de mayo de 2010, Walz (C-63/09, EU:C:2010:251), apartado 21, sobre responsabilidad de los transportistas aéreos, y de 10 de junio de 2021, Van Ameyde España (C-923/19, EU:C:2021:475), apartados 37 y ss., en relación con la responsabilidad civil por accidentes derivados de la circulación de vehículos automóviles.

[34] Por ejemplo, los consumidores de productos o las víctimas de accidentes de tráfico.

[35] En materia de viajes combinados, véase la sentencia de 12 de marzo de 2002, Leitner (C-168/00, EU:C:2002:163); en el ámbito de la responsabilidad civil derivada de la circulación de vehículos automóviles, véanse las sentencias de 24 de octubre de 2013, Haasová (C-22/12, EU:C:2013:692), apartados 47 a 50; de 24 de octubre de 2013, Drozdovs (C-277/12, EU:C:2013:685), apartado 40, y de 23 de enero de 2014, Petillo (C-371/12, EU:C:2014:26), apartado 35.

78. Si bien la jurisprudencia del Tribunal de Justicia autoriza a defender que, en los términos expuestos, existe en el Derecho de la Unión un principio de indemnización de los daños inmateriales, coincido con el Abogado General Campos Sánchez-Bordona en que no puede inferirse de ella una regla en cuya virtud *todo* daño inmaterial sea indemnizable, sea cual sea su seriedad. [36]

79. En este contexto, es pertinente la distinción entre daños inmateriales indemnizables y otros *inconvenientes derivados de la falta de respeto a la legalidad* que, por su escasa entidad, no necesariamente darían derecho a compensación. [37]

80. El Tribunal de Justicia reconoce esta diferencia cuando alude a los trastornos y molestias como categoría autónoma respecto a la de daños, en ámbitos en los que estima que estos deben ser indemnizados. [38]

81. Puede observarse empíricamente que cualquier infracción de una norma sobre protección de datos personales generará alguna reacción negativa del interesado. Una indemnización basada en el mero sentimiento de desagrado ante la falta de respeto de la ley por parte de otros podría confundirse fácilmente con una indemnización sin daño que, como se ha señalado, no parece contemplarse en el supuesto del artículo 82 del Reglamento.

82. El hecho de que, en circunstancias como las del litigio principal, el uso indebido de los datos personales sea solo potencial, y no efectivo, basta para considerar que el interesado puede haber sufrido un daño moral causado por la infracción del Reglamento, siempre que el interesado demuestre que el temor a ese uso indebido le ha ocasionado de forma concreta y específica un daño emocional real y cierto. [39]

[36] Véanse las conclusiones del Abogado General Campos Sánchez-Bordona presentadas en el asunto Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales) (C-300/21, EU:C:2022:756), punto 105. El Tribunal de Justicia ha reconocido, por ejemplo, la compatibilidad con las normas europeas de una ley nacional que, a efectos del cálculo de la indemnización, diferencia los daños inmateriales vinculados a lesiones corporales causadas por un accidente en función del origen de este último; véase el fallo de la sentencia de 23 de enero de 2014, Petillo (C-371/12, EU:C:2014:26), según la cual el Derecho de la Unión no se opone «a una legislación nacional […] que establece un régimen particular de indemnización de los daños inmateriales derivados de lesiones corporales leves causadas por accidentes de tráfico que limita la indemnización de estos daños si se compara con lo aceptado en materia de indemnización de daños idénticos derivados de causas distintas a dichos accidentes».

[37] Esta distinción puede encontrarse en algunos ordenamientos jurídicos nacionales, como corolario inevitable de la vida en sociedad. Recientemente, en materia de protección de datos, en Italia, Tribunale di Palermo, sez. I civile, sentencia de 5.10.2017 n.º 5261, y Cass. Civ., Ord. sez. VI, n.º 17383/2020. En Alemania, entre otras, AG Diez, 7.11.2018 — 8 C 130/18; LG Karlsruhe, 2.08.2019 — 8 O 26/19, y AG Frankfurt am Main, 10.07.2020 — 385 C 155/19 (70). En Austria, OGH 6 Ob 56/21k.

[38] Véase la sentencia de 23 de octubre de 2012, Nelson y otros (C-581/10 y C-629/10, EU:C:2012:657), apartado 51, sobre la distinción entre «daños» en el sentido del artículo 19 del Convenio para la Unificación de Ciertas Reglas para el Transporte Aéreo Internacional, concluido en Montreal el 28 de mayo de 1999, y «molestias» en el sentido del Reglamento (CE) n.º 261/2004 del Parlamento Europeo y del Consejo, de 11 de febrero de 2004, por el que se establecen normas comunes sobre compensación y asistencia a los pasajeros aéreos en caso de denegación de embarque y de cancelación o gran retraso de los vuelos, y se deroga el Reglamento (CEE) n.º 295/91 (DO 2004, L 46, p. 1), que son indemnizables al amparo del artículo 7 de este último a tenor de la sentencia de 19 de noviembre de 2009, Sturgeon y otros (C-402/07 y C-432/07, EU:C:2009:716). En este sector, como en el del transporte de pasajeros por mar y vías navegables al que se refiere el Reglamento (UE) n.º 1177/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, sobre los derechos de los pasajeros que viajan por mar y por vías navegables y por el que se modifica el Reglamento (CE) n.º°2006/2004 (DO 2010, L 334, p. 1), el legislador ha podido reconocer una categoría abstracta gracias a que el factor que genera el trastorno y la esencia de este son idénticos para todos los afectados. No creo que esa inferencia resulte posible en materia de protección de datos.

[39] Según Irlanda, estas consideraciones son especialmente importantes en la práctica en el contexto de la ciberdelincuencia, ya que si toda persona afectada —aunque solo sea mínimamente— por una infracción tuviera derecho a una indemnización de los daños inmateriales, el impacto consiguiente sería intenso, en particular en los responsables del tratamiento de datos del sector público, que son financiados con fondos públicos limitados y deben servir a intereses colectivos, incluida la mejora de la seguridad de los datos personales (observaciones escritas, apartado 72).

83. La frontera entre las meras contrariedades (no indemnizables) y los verdaderos daños inmateriales (indemnizables) es ciertamente tenue, pero los jueces nacionales, a quienes corresponde la tarea de delimitar esa frontera caso por caso, deben realizar una apreciación cuidadosa de todos los elementos aportados por el interesado que solicita la indemnización, a quien incumbirá la carga de alegar con precisión, y no de modo genérico, elementos concretos que puedan llevar a apreciar un «daño moral efectivamente sufrido» a causa de la violación de la seguridad de los datos personales, sin alcanzar, no obstante, un umbral predeterminado de especial gravedad. Lo que importa es que no se trate de una simple percepción subjetiva, cambiante y dependiente también de factores personales y de carácter, sino que sea un trastorno objetivo, incluso de carácter leve pero que sea comprobable, de su esfera física o psíquica o de sus relaciones, la naturaleza de los datos personales de que se trate y la importancia que revisten en la vida del interesado y quizás también la percepción que, en ese momento, tenga la sociedad de ese trastorno concreto derivado de la violación de la seguridad de los datos. [40]

IV. Conclusión

84. Habida cuenta de las consideraciones antes expuestas, propongo al Tribunal de Justicia que responda del siguiente modo a las cuestiones prejudiciales planteadas:

«Los artículos 5, 24, 32 y 82 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

la mera existencia de una "violación de la seguridad de los datos personales", tal como se define en el artículo 4, apartado 12, no basta por sí sola para concluir que las medidas técnicas y organizativas aplicadas por el responsable del tratamiento no eran "apropiadas" para garantizar la protección de los datos en cuestión;

al examinar la adecuación de las medidas técnicas y organizativas aplicadas por el responsable del tratamiento de los datos personales, el juez nacional que conoce del asunto debe realizar un control que comprenda un análisis concreto tanto del contenido de las medidas como del modo en que se han aplicado y sus efectos prácticos;

en el marco de una demanda de indemnización de daños con arreglo al artículo 82 del Reglamento General de Protección de Datos, el responsable del tratamiento de los datos personales tiene la carga de probar la adecuación de las medidas que ha aplicado con arreglo al artículo 32 de dicho Reglamento;

de conformidad con el principio de autonomía procesal, corresponde al ordenamiento jurídico interno de cada Estado miembro determinar los medios de prueba admisibles y su valor probatorio, incluidas las diligencias de prueba que los tribunales nacionales pueden o deben ordenar para dilucidar si el responsable del tratamiento de los datos personales ha adoptado medidas apropiadas con arreglo al citado Reglamento, respetando los principios de equivalencia y de eficacia establecidos en el Derecho de la Unión;

[40] Véanse las conclusiones del Abogado General Campos Sánchez-Bordona presentadas en el asunto Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales) (C-300/21, EU:C:2022:756), punto 116.

el hecho de que la infracción del citado Reglamento causante del daño en cuestión haya sido cometida por un tercero no constituye en sí mismo un motivo para eximir de responsabilidad al responsable del tratamiento y, a fin de acogerse a la exención prevista por esa disposición, el responsable del tratamiento debe demostrar que no es en modo alguno responsable de la infracción;

el perjuicio consistente en el temor a un potencial futuro uso indebido de sus datos personales, cuya existencia haya sido demostrada por el interesado, puede constituir un daño moral que genere derecho a indemnización, siempre que el interesado demuestre que ha sufrido individualmente un daño emocional real y cierto, lo cual corresponderá comprobar en cada caso concreto al juez nacional que conoce del asunto.»