Asunto C-340/21

Resumen de la petición de decisión prejudicial con arreglo al artículo 98, apartado 1, del Reglamento de Procedimiento del Tribunal de Justicia

Fecha de presentación:

2 de junio de 2021

Órgano jurisdiccional remitente:

Varhoven administrativen sad (Tribunal Supremo de lo Contencioso-Administrativo, Bulgaria)

Fecha de la resolución de remisión:

14 de mayo de 2021

Parte recurrente en casación:

VB

Parte recurrida en casación:

Natsionalna agentsia za prihodite (Agencia Nacional de Recaudación)

Objeto del procedimiento principal

Recurso interpuesto contra una sentencia por la cual se desestimó por infundada la acción indemnizatoria de daños inmateriales ocasionados por el incumplimiento ilícito de la parte recurrida en casación en su condición de responsable del tratamiento, de las obligaciones que le incumben en virtud de la Zakon za zashtita na lichnite danni (Ley de protección de los datos personales) y del Reglamento 2016/679.

Objeto y fundamento jurídico de la petición de decisión prejudicial

Petición de decisión prejudicial planteada en virtud del artículo 267 TFUE, que tiene por objeto la interpretación de los considerandos 74, 85 y 146 y los artículos 4, punto 12; 5, apartado 2; 24, 32 y 82 del Reglamento 2016/679.

Cuestiones prejudiciales

1) ¿Deben interpretarse los artículos 24 y 32 del Reglamento (UE) 2016/679 en el sentido de que, cuando se ha producido una divulgación no autorizada o un acceso no autorizado a datos personales a efectos del artículo 4, punto 12, del Reglamento (UE) 2016/679 por personas que no son funcionarios de la administración del responsable del tratamiento y no están sometidas al control de este, basta 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 (UE) 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 (UE) 2016/679 en el sentido de que en el procedimiento indemnizatorio con arreglo al artículo 82, apartado 1, del Reglamento (UE) 2016/679 le incumbe al responsable del tratamiento la carga de la prueba de haber adoptado medidas técnicas y organizativas apropiadas a efectos del artículo 32 del 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 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 (UE) 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 (UE) 2016/679, como en el presente caso, mediante un «ciberataque», por personas que no son empleados de la administración del responsable y no están sometidas al control de este, constituye un hecho del cual en modo alguno debe responder 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 (UE) 2016/679 en el sentido de que, en un caso como el presente, en 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, la sola preocupación, temor y miedo del interesado respecto a un posible uso indebido de sus datos personales en el futuro quedan comprendidos en el concepto de daños inmateriales, que ha de ser interpretado en sentido amplio, y fundamenta una pretensión indemnizatoria, aunque no se haya constatado tal uso indebido y/o el interesado no haya sufrido ningún otro perjuicio?

Jurisprudencia y disposiciones de la Unión invocadas

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; en lo sucesivo, «Reglamento»): Considerandos 1, 4, 6, 74, 75, 76, 77, 83, 85 y 146; artículos 4, puntos 2, 7 y 12; 5, 24, 32, 33, 79 y 82

Sentencia del Tribunal de Justicia de 30 de mayo de 2013, Worten (C-342/12, EU:C:2013:355), apartados 24 y 26

Disposiciones de Derecho nacional invocadas

Administrativnoprotsesualen kodeks (Ley del procedimiento contencioso-administrativo): artículos 144, apartado 1; 203 y 208

Grazhdanski protsesualen kodeks (Ley de enjuiciamiento civil): artículo 154

Zakon za otgovornostta na darzhavata i obshtinite za vredi (Ley de responsabilidad indemnizatoria del Estado y de los municipios): artículo 1

Zakon za zashtita na lichnite danni (Ley de protección de los datos personales): artículos 39, apartados 1 y 2, y 59, apartado 1

Breve exposición de los hechos y del procedimiento principal

1 La Natsionalna agentsia po prihodite (Agencia Nacional de Recaudación; en lo sucesivo, «NAP») es responsable del tratamiento en el sentido del artículo 4, punto 7, del Reglamento. Con arreglo al Derecho nacional, se trata de un organismo especializado dependiente del Ministro de Hacienda y al que le compete determinar, afianzar y cobrar los créditos del Estado de carácter público y los de carácter privado que establezca la ley. En el cumplimiento de las facultades públicas que tiene atribuidas, trata datos personales.

2 El 15 de julio de 2019, los medios de comunicación búlgaros informaron al público en general de un acceso no autorizado al sistema informático de la NAP, a raíz del cual se habían publicado en Internet informaciones procedentes de sus bases de datos que contenían datos personales y datos relativos a impuestos y seguridad social. Se vieron afectados 4 057 328 ciudadanos búlgaros, y el número de personas físicas afectadas, incluidas tanto las de nacionalidad búlgara como extranjera, ascendió a 6 074 140. Entre ellas figuraba VB.

3 Hasta la fecha, no se ha dictado ninguna sentencia penal firme contra las personas que [presuntamente] cometieron el acceso no autorizado, calificado en los medios como «ciberataque».

4 Tras el acceso, cientos de ciudadanos demandaron a la NAP reclamándole una indemnización por los daños inmateriales sufridos.

5 El 16 de septiembre de 2019, VB presentó una demanda contra la NAP ante el Administrativen sad Sofía-grad (Tribunal de lo Contencioso-Administrativo de la ciudad de Sofía; en lo sucesivo, «ASSG»), reclamando una indemnización de 1 000 BGN (aproximadamente 511 euros) con arreglo al artículo 82, apartado 1, del Reglamento, al artículo 1, apartado 1, de la Zakon za otgovornostta na darzhavata i obshtinite za vredi (Ley de responsabilidad indemnizatoria del Estado y de los municipios) y al artículo 39, apartado 1, de la Zakon za zashtita na lichnite danni (Ley de protección de los datos personales).

6 En su demanda en primera instancia, VB alegó que la NAP no había cumplido «de la mejor manera posible» sus obligaciones de «mantener una impecable ciberseguridad» y de «garantizar efectivamente el mayor grado de seguridad de los datos personales de los ciudadanos de la República de Bulgaria». Como consecuencia de ello, se había producido una violación de la seguridad de los datos personales a efectos del artículo 4, punto 12, del Reglamento y los datos personales habían sido divulgados ilegalmente.

7 VB consideraba que «la falta de diligencia y la omisión de unas medidas efectivas de protección de datos» debía considerarse un incumplimiento de las obligaciones que incumben a la NAP respecto a la protección de los datos de los ciudadanos, lo que constituía una infracción de los artículos 24 y 32 del Reglamento. Como responsable del tratamiento, la NAP estaba obligada a tratar los datos personales de tal manera que se «garanti[zase] una seguridad adecuada» mediante la adopción de medidas técnicas y organizativas apropiadas.

8 VB alegó que el incumplimiento de la NAP le había ocasionado un daño inmaterial que se traducía en inquietudes y temores acerca del futuro uso indebido de sus datos personales, por ejemplo, para sustraer sus bienes, utilizar indebidamente sus cuentas bancarias, contratar créditos en su nombre, modificar su estado civil o usurpar su identidad. Afirmaba sentirse indignada por «tamaña intrusión en el sistema informático de la NAP» y desamparada por el Estado. Tenía miedo de ser extorsionada, agredida o sufrir un secuestro.

9 La NAP consideró que la demanda era infundada. VB no le había solicitado información alguna acerca de los datos personales concretos a los que se había accedido.

10 La NAP señala que, tras el acceso, adoptó medidas con carácter inmediato para proteger los derechos e intereses de los ciudadanos. Celebró reuniones con representantes y expertos de los servicios de seguridad, de la Notarialna kamara (Colegio Notarial), de la Agentsia po vpisvaniata (Agencia de Registros), de la Asotsiatsia na targovskite banki (Federación de Bancos Comerciales), etc., para coordinar las medidas tendentes a reducir los efectos de la intrusión. En la página

web de la NAP se incluyeron apartados específicos relativos al ciberataque en los que se publicó información actualizada al respecto.

11 En opinión de la NAP, no existe una relación de causalidad entre los supuestos daños inmateriales y el acceso no autorizado a los datos personales. La NAP fue víctima de un ataque deliberado por parte de terceros ajenos al organismo, por lo que no se la puede hacer responsable de los daños producidos.

12 La NAP afirma haber adoptado numerosas medidas. En concreto, introdujo sistemas de gestión de procesos y sistemas de gestión de seguridad, autorizó procedimientos conformes con las normas internacionales de calidad ISO 9000 e ISO 9001 e introdujo directrices, normas, procesos, instrucciones y métodos de gestión de la seguridad informática.

13 La NAP aportó pruebas (a saber, diversos documentos internos correspondientes al período comprendido entre enero de 2013 y mayo de 2019) sobre el contenido y el proceso de recogida, mantenimiento y acceso a las bases de datos; la introducción de sistemas de gestión de la seguridad informática; los procedimientos de prevención; las normas internas de seguridad informática y de redes; las instrucciones impartidas sobre el manejo de la información; las directrices para la protección de los datos personales; las medidas y medios dispuestos para proteger los datos personales, y los métodos y procedimientos de evaluación de riesgos.

14 Mediante sentencia de 27 de noviembre de 2020, el ASSG desestimó la demanda de VB por infundada.

15 El ASSG señaló que el acceso no autorizado a la base de datos de la NAP mediante un «ciberataque» fue llevado a cabo por personas contra las cuales se habían iniciado diligencias de investigación que aún estaban en curso.

16 Del resultado ilícito no se podía deducir que el responsable del tratamiento no hubiese cumplido con sus obligaciones de adoptar medidas técnicas y organizativas apropiadas para garantizar la protección de la base de datos de modo que nadie pudiese acceder nunca a ella de ninguna manera y por ningún medio.

17 El ASSG consideró que la demandante debía señalar las actuaciones (técnicas) que hubiera debido emprender efectivamente la NAP y no emprendió o no lo hizo correctamente, a causa de lo cual se produjo el resultado del acceso no autorizado y la divulgación de los datos personales, o cómo contribuyó la NAP a la producción de este resultado.

18 En opinión del ASSG, a la vista de los elementos de prueba presentados no cabía apreciar omisión alguna por parte del responsable del tratamiento. A VB no se le había causado ningún daño inmaterial susceptible de resarcimiento. El sufrimiento psicológico experimentado a consecuencia de la noticia del acceso no autorizado a las bases de datos de la NAP era un fenómeno normal, pero no constituía un perjuicio real desde el punto de vista jurídico. VB no había tratado de averiguar

exactamente cuáles de sus datos personales habían sido objeto del acceso, y este comportamiento no permitía apreciar una profunda angustia emocional.

19 El ASSG concluyó que la comunicación al público del acceso ilegal sufrido por la base de datos de la NAP no había tenido consecuencias para la vida de VB en cuanto a su amor propio, su autoestima, su trabajo, sus relaciones ni su estado de salud. No existe relación causal alguna con las emociones negativas experimentadas, pues estas no eran el resultado del comportamiento de la NAP.

20 VB recurrió la sentencia del ASSG ante el órgano jurisdiccional remitente, el Varhoven administrativen sad (Tribunal Supremo de lo Contencioso-Administrativo; en lo sucesivo, «VAS»).

Alegaciones esenciales de las partes en el procedimiento principal

21 En su recurso de casación, VB alega que el ASSG hizo un reparto incorrecto de la carga de la prueba respecto a un hecho negativo, concretamente la omisión por parte del responsable del tratamiento de las medidas técnicas y organizativas apropiadas.

22 VB considera que la adopción de medidas apropiadas queda a criterio de la NAP, de manera que no es posible señalar las obligaciones concretas que deberían haber cumplido y omitieron cumplir los funcionarios de la NAP. Los elementos de prueba aportados por la NAP no demostraban que las medidas técnicas y organizativas adoptadas fuesen apropiadas.

23 En opinión de VB, las inquietudes acerca de un eventual uso indebido de sus datos personales en el futuro no constituyen daños hipotéticos, sino daños inmateriales efectivos susceptibles de resarcimiento. Entiende que no es necesario acreditar un daño inmaterial normal.

24 La NAP entiende que el ASSG consideró acertadamente que, en su condición de responsable del tratamiento, no cometió omisión alguna, sino que adoptó numerosas medidas técnicas y organizativas para proteger los datos personales durante su tratamiento. Asimismo, alega que no se ha acreditado la producción efectiva de un daño. Las inquietudes y el temor ante acontecimientos futuros no son indemnizables.

Breve exposición de la fundamentación de la petición de decisión prejudicial

25 Otros procedimientos similares contra la NAP concluyeron en primera instancia con resultados contradictorios. En algunos casos, las demandas fueron desestimadas por infundadas; en otros, fueron estimadas total o parcialmente. La legislación fue interpretada y aplicada de forma contradictoria en cuanto a todos los elementos de la responsabilidad del responsable del tratamiento.

26 El VAS considera que el supuesto de hecho de la responsabilidad con arreglo al artículo 82 del Reglamento comprende los siguientes elementos: i) una infracción del Reglamento por parte del responsable; ii) daños materiales o inmateriales sufridos por el interesado, y iii) una relación de causalidad entre los daños sufridos y la infracción concreta.

Primera cuestión prejudicial

27 Con arreglo al artículo 24, apartado 1, del Reglamento, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

28 El artículo 32 del Reglamento impone al responsable obligaciones relativas a la seguridad del tratamiento, obligaciones que son relevantes para su responsabilidad en virtud del artículo 24 y que la desencadenan. Se enumeran allí los criterios que han de regir la adopción de las medidas técnicas y organizativas apropiadas para garantizar un nivel de protección adecuado a los riesgos existentes. Entre dichos criterios figuran «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».

29 El Reglamento no define el concepto de «medidas técnicas y organizativas apropiadas». En su considerando 74 se indica que 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 Reglamento, incluida la eficacia de las medidas.

30 De lo anterior se deduce que el responsable ha de llevar a cabo una evaluación de los riesgos conforme a los criterios establecidos en el artículo 32 del Reglamento, criterios que han de guiar las medidas técnicas y organizativas adoptadas, las cuales deben ser apropiadas en relación con el nivel de protección de los datos personales necesario y adecuado a los riesgos. Con la introducción de medidas técnicas y organizativas apropiadas, el responsable se asegura de tratar los datos personales de conformidad con el Reglamento.

31 De las citadas disposiciones se desprende que la elección de las medidas técnicas y organizativas apropiadas es una cuestión de oportunidad. Sin embargo, la valoración de la oportunidad por el responsable no está sujeta a control judicial, pues los tribunales únicamente controlan la legalidad. Por otro lado, habida cuenta del margen de apreciación existente para la elección de las medidas técnicas y organizativas, el tratamiento de datos personales debe ser conforme con el Reglamento y con el objetivo que este persigue de salvaguardar el derecho fundamental a la protección de los datos personales.

32 Partiendo de las consideraciones que preceden, el VAS solicita que se aclare si los artículos 24 y 32 del Reglamento se han de interpretar en el sentido de que la sola materialización del resultado ilícito consistente en la divulgación no autorizada de datos personales o en el acceso no autorizado a estos a efectos del artículo 4, punto 12, del Reglamento sirve como prueba de que el responsable del tratamiento no adoptó las medidas técnicas y organizativas apropiadas.

Segunda cuestión prejudicial (en caso de respuesta negativa a la primera cuestión)

33 Dado que la elección y aplicación de las medidas técnicas y organizativas se ha dejado a la valoración subjetiva del responsable del tratamiento y queda sujeta al margen de apreciación de este, al VAS se le plantea la cuestión de cuál ha de ser el objeto y alcance del control judicial de legalidad al examinar si las medidas técnicas y organizativas adoptadas por el responsable del tratamiento fueron apropiadas y conformes con los artículos 24 y 32 del Reglamento.

34 El VAS alberga dudas acerca de si basta con que el tribunal aclare en qué medida el responsable cumplió con las obligaciones que le incumben en virtud de las citadas disposiciones, o si debe examinar el contenido de las medidas técnicas y organizativas elegidas y aplicadas, a pesar de que estas solamente se mencionan con carácter ejemplificativo en el Reglamento y se han de aplicar en función de su oportunidad.

Tercera cuestión prejudicial (en caso de respuesta negativa a la primera cuestión)

35 Con arreglo al artículo 5, apartado 2, del Reglamento, le incumbe al responsable del tratamiento el cumplimiento de los principios del apartado 1 de dicha disposición relativos al tratamiento de los datos personales, y debe ser capaz de demostrar dicho cumplimiento. El artículo 24, apartado 1, del Reglamento impone al responsable del tratamiento la obligación de aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

36 El artículo 82, apartado 3, del Reglamento permite al responsable o al encargado del tratamiento exonerarse de su responsabilidad en virtud del apartado 2 «si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios». Con arreglo al mencionado apartado 2, el responsable responderá de los daños y perjuicios causados en caso de que el tratamiento no cumpla lo dispuesto por el Reglamento.

37 De conformidad con la legislación nacional, corresponde a cada parte procesal demostrar los hechos de los cuales se deducen sus pretensiones u objeciones. En los procedimientos similares, los tribunales de primera instancia han repartido de forma diversa la carga de la prueba entre el demandante y el demandado.

38 En el presente asunto resulta relevante la cuestión de si el principio de responsabilidad proactiva del artículo 5, apartado 2, en relación con el considerando 74 y el artículo 24, apartado 1, del Reglamento se debe interpretar en el sentido de que invierte la carga de la prueba y, por tanto, le incumbe al responsable del tratamiento contra el que se dirige una acción indemnizatoria por una infracción del Reglamento, como demandado, demostrar que las medidas técnicas y organizativas que aplicó eran apropiadas.

39 Aparte de la cuestión del objeto y alcance del control judicial del cumplimiento de las obligaciones derivadas del Reglamento, cabe preguntarse también cómo ha de examinarse, y atendiendo a qué elementos de prueba, si se cumplieron dichas obligaciones y, en particular, si se adoptaron todas las medidas técnicas y organizativas apropiadas.

40 En el procedimiento, la NAP ha presentado pruebas relativas a la garantía de la protección de las redes de información de conformidad con los métodos indicados en los documentos, pero no se ha recabado ningún dictamen pericial técnico-forense para determinar si las medidas técnicas y organizativas adoptadas fueron apropiadas en el sentido del Reglamento. El VAS es consciente de que un responsable como la NAP está obligado a aplicar medidas organizativas, tecnológicas y técnicas para garantizar la seguridad informática y de redes, que guarden una relación adecuada con las amenazas de la ciberdelincuencia, a fin de reducir al mínimo el riesgo de su materialización. Sin embargo, el acceso por parte de los peritos forenses en cada procedimiento basado en el artículo 82 del Reglamento acarrearía nuevas consecuencias negativas para la protección de los datos personales.

41 Teniendo en cuenta el estado de la técnica, los actuales métodos de protección de los sistemas de redes de información y el acceso no autorizado que se produjo mediante un «ciberataque» perpetrado por personas ajenas a la administración del responsable, el VAS se plantea la cuestión de si recabar un dictamen pericial técnico-forense puede considerarse una prueba necesaria y suficiente para determinar si las medidas técnicas y organizativas elegidas y aplicadas fueron apropiadas para garantizar la protección de los datos personales.

Cuarta cuestión prejudicial

42 Como responsable que participa en la operación de tratamiento, la NAP responde de los daños, pero puede quedar exenta de la responsabilidad en virtud del artículo 82, apartado 3, si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

43 En el presente procedimiento no es objeto de debate que el acceso a los datos personales tuvo lugar por medio de un «ciberataque» contra la NAP. En cambio, el acceso no autorizado y la divulgación de los datos personales no se produjeron con motivo o a causa del tratamiento de dichos datos por los funcionarios de la NAP.

44 El VAS solicita que se aclare si en el presente caso es posible considerar que se trata de hechos de los cuales no es en modo alguno responsable el responsable del tratamiento, por lo cual este queda exento de responsabilidad.

Quinta cuestión prejudicial

45 La interesada reclama la indemnización de los daños inmateriales sufridos, consistentes en inquietud, miedo, estrés, sentimiento de inseguridad y temor de un futuro uso indebido de sus datos personales de las distintas formas por ella descritas. No hay ningún motivo para considerar que los datos personales de VB hayan sido objeto de un uso indebido.

46 Según se deduce de los considerandos 75 y 85 del Reglamento, la enumeración de ejemplos de daños materiales e inmateriales tiene en cuenta el tipo de datos personales y los efectos adversos para los interesados, y no sus simples sentimientos subjetivos.

47 En el considerando 146 del Reglamento se establecen los límites de la responsabilidad: Esta comprende los «daños y perjuicios» que pueda sufrir una persona como consecuencia de un tratamiento en infracción del Reglamento.

48 Después de haberse producido ya un acceso, los datos personales del interesado pueden ser objeto de numerosos usos indebidos de naturaleza material o inmaterial, con graves consecuencias. Tales casos de uso indebido han llegado a conocimiento del público, lo cual puede justificar una preocupación aún mayor para las personas afectadas por el «ciberataque». En el presente caso, a falta de datos sobre un uso indebido ya cometido, la posibilidad de un futuro uso indebido no es sino una mera suposición, la hipótesis de un riesgo posible, aunque incierto, para los derechos de la interesada.

49 Por las razones antes expuestas se plantea la cuestión de si los sentimientos negativos de la interesada a este respecto, es decir, si el solo hecho de padecer el miedo a un posible uso indebido de los datos personales en el futuro, está comprendido en el concepto de daños inmateriales, que ha de ser interpretado en sentido amplio, y constituye una causa de indemnización con arreglo al artículo 82, apartado 1, en relación con el considerando 146 del Reglamento.

50 No obstante, es posible que el artículo 82, apartado 1, en relación con el considerando 146 del Reglamento no pueda interpretarse en el sentido de que cualquier sentimiento negativo, miedo o inquietud por parte del interesado fundamente su derecho a un resarcimiento del daño inmaterial sufrido si previamente no se ha producido una utilización ilícita, como pueden ser la sustracción de bienes, la contratación de créditos a nombre del interesado o la usurpación de su identidad.