



Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Sala Tercera)

de 11 de diciembre de 2019*

«Procedimiento prejudicial — Protección de las personas físicas en lo que respecta al tratamiento de datos personales — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7 y 8 — Directiva 95/46/CE — Artículos 6, apartado 1, letra c), y 7, letra f) — Legitimación del tratamiento de datos personales — Normativa nacional que permite la videovigilancia para garantizar la seguridad y la protección de las personas, bienes y activos y la satisfacción de intereses legítimos sin el consentimiento del interesado — Instalación de un sistema de videovigilancia en las zonas comunes de un inmueble de uso residencial»

En el asunto C-708/18,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por el Tribunalul București (Tribunal de Distrito de Bucarest, Rumanía), mediante resolución de 2 de octubre de 2018, recibida en el Tribunal de Justicia el 6 de noviembre de 2018, en el procedimiento entre

TK

y

Asociația de Proprietari bloc M5A-ScaraA,

EL TRIBUNAL DE JUSTICIA (Sala Tercera),

integrado por la Sra. A. Prechal (Ponente), Presidenta de Sala, y la Sra. L. S. Rossi, y los Sres. J. Malenovský, F. Biltgen y N. Wahl, Jueces;

Abogado General: Sr. G. Pitruzzella;

Secretario: Sr. A. Calot Escobar;

habiendo considerado los escritos obrantes en autos;

consideradas las observaciones presentadas:

- en nombre del Gobierno rumano, por el Sr. C.-R. Canțăr y las Sras. O.-C. Ichim y A. Wellman, en calidad de agentes;
- en nombre del Gobierno checo, por los Sres. M. Smolek, J. Vlácil y O. Serdula, en calidad de agentes;

* Lengua de procedimiento: rumano.

- en nombre del Gobierno danés, por el Sr. J. Nymann-Lindegren y las Sras. M. Wolff y P. Ngo, en calidad de agentes;
- en nombre de Irlanda, por las Sras. M. Browne y G. Hodge y el Sr. A. Joyce, en calidad de agentes, asistidos por el Sr. D. Fenelly, BL;
- en nombre del Gobierno austriaco, inicialmente por el Sr. G. Hesse y la Sra. J. Schmoll, y posteriormente por la Sra. Schmoll, en calidad de agentes;
- en nombre del Gobierno portugués, por el Sr. L. Inez Fernandes y las Sras. P. Barros da Costa, L. Medeiros, I. Oliveira y M. Cancela Carvalho, en calidad de agentes;
- en nombre de la Comisión Europea, por los Sres. H. Kranenborg y D. Nardi y la Sra. L. Nicolae, en calidad de agentes;

vista la decisión adoptada por el Tribunal de Justicia, oído el Abogado General, de que el asunto sea juzgado sin conclusiones;

dicta la siguiente

Sentencia

- 1 La petición de decisión prejudicial tiene por objeto la interpretación de los artículos 6, apartado 1, letra e), y 7, letra f), de 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), así como de los artículos 8 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).
- 2 Esta petición se ha formulado en el contexto de un litigio entre TK y la AsociaȚia de Proprietari bloc M5A-Scara A (Comunidad de Propietarios del Bloque M5A-Escalera A, Rumanía; en lo sucesivo, «comunidad de propietarios»), en relación con la demanda presentada por TK para que dicha comunidad desactivara el sistema de videovigilancia de ese edificio y retirara las cámaras instaladas en las zonas comunes del mismo.

Marco jurídico

Derecho de la Unión

- 3 La Directiva 95/46 fue derogada y sustituida, con efectos a partir del 25 de mayo de 2018, por el 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 (DO 2016, L 119, p. 1). Sin embargo, el litigio principal se rige por las disposiciones de la citada Directiva, habida cuenta de la fecha en la que sucedieron los hechos de que se trata.
- 4 La Directiva 95/46 tenía por objeto, según su artículo 1, la protección de las libertades y de los derechos fundamentales de las personas físicas, en particular del derecho a la vida privada, en lo que respecta al tratamiento de los datos personales, y la eliminación de los obstáculos a la libre circulación de tales datos.

5 El artículo 3 de esta Directiva establecía, en su apartado 1, lo siguiente:

«Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.»

6 El capítulo II de dicha Directiva incluía una sección I, titulada «Principios relativos a la calidad de los datos» e integrada por su artículo 6, que establecía lo siguiente:

«1. Los Estados miembros dispondrán que los datos personales sean:

- a) tratados de manera leal y lícita;
- b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;
- c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas;
- e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.»

7 En la sección II de dicho capítulo II, titulada «Principios relativos a la legitimación de las operaciones de tratamiento de datos», el artículo 7 de la Directiva 95/46 tenía el siguiente tenor:

«Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

- a) el interesado ha dado su consentimiento de forma inequívoca, o
- b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
- c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- d) es necesario para proteger el interés vital del interesado, o
- e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

- f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.»

Derecho rumano

- 8 La Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Ley n.º 677/2001 para la Protección de las Personas en relación con el Tratamiento de los Datos Personales y la Libre Circulación de Tales Datos; *Monitorul Oficial al României*, parte I, n.º 790, de 12 de diciembre de 2001), en su versión modificada por la Ley n.º 102/2005 y por el Decreto-ley con carácter de urgencia n.º 36/2007, aplicable *ratione temporis* al litigio principal, fue adoptada con el fin de transponer al Derecho rumano la Directiva 95/46.
- 9 El artículo 5 de esta Ley disponía lo siguiente:
- «(1) Todo tratamiento de datos personales, a menos que se refiera a datos pertenecientes a las categorías mencionadas en los artículos 7, apartado 1, 8 y 10, solo podrá llevarse a cabo si el interesado ha prestado expresa e inequívocamente su consentimiento para dicho tratamiento.
- (2) El consentimiento del interesado no se requerirá en los siguientes casos:
- a) cuando el tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el interesado sea parte o para la adopción de medidas, a petición del interesado, antes de la celebración de un contrato o precontrato;
- b) cuando el tratamiento sea necesario para la protección de la vida, la integridad física o la salud del interesado o de otra persona amenazada;
- c) cuando el tratamiento sea necesario para el cumplimiento de una obligación legal del responsable del tratamiento;
- d) cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o al tercero a quien se comuniquen los datos;
- e) cuando el tratamiento sea necesario para la satisfacción de un interés legítimo del responsable del tratamiento o del tercero a quien se comuniquen los datos, siempre que dicho interés no perjudique el interés o los derechos y libertades fundamentales del interesado;
- f) cuando el tratamiento se refiera a datos procedentes de documentos accesibles al público, de conformidad con la ley;
- g) cuando el tratamiento se realice exclusivamente con fines estadísticos, históricos o de investigación científica y los datos sigan siendo anónimos durante todo el tratamiento.
- (3) Lo dispuesto en el apartado 2 se entenderá sin perjuicio de las disposiciones legales que regulan la obligación de las autoridades públicas de respetar y proteger la vida personal, familiar y privada.»
- 10 La Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video [Decisión de la Autoridad Nacional de Supervisión del Tratamiento de Datos

Personales (en lo sucesivo, «Autoridad de Supervisión del Tratamiento de Datos») n.º 52/2012, relativa al tratamiento de los datos personales mediante videovigilancia], en su versión aplicable al litigio principal, establecía lo siguiente en su artículo 1:

«Constituirán operaciones de tratamiento de datos personales que entran en el ámbito de aplicación de la [Ley 677/2001] la recogida, grabación, almacenamiento, utilización, transmisión, divulgación o cualquier otra operación de tratamiento de imágenes por medios de videovigilancia que permita, directa o indirectamente, la identificación de las personas físicas.»

11 El artículo 4 de dicha Decisión disponía lo siguiente:

«La videovigilancia podrá emplearse, con carácter principal, con los siguientes fines:

- a) la prevención y la lucha contra el delito;
- b) la vigilancia de la circulación vial y la detección de infracciones de las normas de tráfico;
- c) el cuidado y la protección de las personas, bienes y activos y de los edificios e instalaciones de utilidad pública así como de sus recintos;
- d) la ejecución de medidas de interés público o el ejercicio de prerrogativas de los poderes públicos;
- e) la satisfacción de intereses legítimos, siempre que no se vulneren los derechos y libertades fundamentales de los interesados.»

12 A tenor del artículo 5, apartados 1 a 3, de la citada Decisión:

«(1) La videovigilancia podrá emplearse en los lugares y espacios abiertos o destinados al público, incluidas las vías públicas de acceso situadas en dominio público o privado, con sujeción a la ley.

(2) Las cámaras de videovigilancia se instalarán en lugares visibles.

(3) Se prohíbe el uso de medios ocultos de videovigilancia, salvo en los casos legalmente autorizados.»

13 El artículo 6 de la misma Decisión disponía lo siguiente:

«El tratamiento de datos personales mediante sistemas de videovigilancia se efectuará con el consentimiento expreso e inequívoco del interesado o en los casos establecidos en el artículo 5, apartado 2, de la Ley n.º 677/2001 [...]».

Litigio principal y cuestiones prejudiciales

14 TK reside en un apartamento de su propiedad situado en el edificio M5A. A petición de algunos copropietarios de ese edificio, la comunidad de propietarios aprobó, en una junta general celebrada el 7 de abril de 2016, la decisión de instalar cámaras de videovigilancia en el edificio.

15 En ejecución de esa decisión, se instalaron tres cámaras de videovigilancia en las zonas comunes del edificio M5A. La primera cámara se orientó hacia la fachada del edificio, mientras que la segunda y la tercera se colocaron, respectivamente, en el vestíbulo de la planta baja y en el ascensor del edificio.

16 TK se opuso a la instalación de este sistema de videovigilancia, al considerar que violaba el derecho al respeto de la vida privada.

- 17 Tras comprobar que dicho sistema de videovigilancia seguía en funcionamiento pese a sus numerosas iniciativas en contra de ello y al reconocimiento de la ilegalidad del mismo por parte de la comunidad de propietarios, TK presentó ante el órgano jurisdiccional remitente una demanda para que obligara a la comunidad a retirar las tres cámaras y a desactivarlas definitivamente, so pena de multa.
- 18 Ante dicho órgano jurisdiccional, TK alegó que el sistema de videovigilancia en cuestión infringía el Derecho originario y derivado de la Unión, en particular el derecho al respeto de la vida privada, así como el Derecho nacional relativo al derecho al respeto de la vida privada. Añadió que la comunidad de propietarios había asumido la función de responsable del tratamiento de los datos personales obviando el procedimiento de registro legalmente previsto a tal efecto.
- 19 La comunidad de propietarios indicó que la decisión de instalar un sistema de videovigilancia se había adoptado para controlar de la manera más efectiva posible las entradas y salidas del edificio, ya que el ascensor había sido vandalizado en varias ocasiones y varios apartamentos y zonas comunes habían sido objeto de allanamientos y robos.
- 20 Precisó, además, que otras medidas que había adoptado anteriormente, a saber, la instalación de un sistema de entrada al edificio con interfono y tarjeta magnética, no habían impedido la comisión reiterada de delitos de la misma naturaleza.
- 21 La comunidad de propietarios también remitió a TK el acta levantada en presencia de la empresa que había instalado las cámaras del sistema de videovigilancia, que indicaba que el 21 de octubre de 2016 se había procedido al borrado y a la desconexión del disco duro del sistema, que este último se había desactivado y que las imágenes grabadas habían sido eliminadas.
- 22 También le remitió otra acta de 18 de mayo de 2017, según la cual las tres cámaras de videovigilancia habían sido desinstaladas. Esta acta precisaba que, entretanto, la comunidad de propietarios había tramitado el procedimiento de registro como responsable del tratamiento de datos personales.
- 23 Sin embargo, TK señaló ante órgano jurisdiccional remitente que las tres cámaras de videovigilancia seguían instaladas.
- 24 El órgano jurisdiccional remitente pone de manifiesto que el artículo 5 de la Ley n.º 677/2001 dispone, de manera general, que el tratamiento de datos personales, como la grabación de imágenes mediante un sistema de videovigilancia, solo puede llevarse a cabo con el consentimiento expreso e inequívoco del interesado. Sin embargo, el apartado 2 del mismo artículo establece una serie de excepciones a esta regla, entre las que figura la referente a la necesidad del tratamiento de datos para la protección de la vida, la integridad física o la salud del interesado o de otra persona amenazada. La Decisión n.º 52/2012 de la Autoridad de Supervisión del Tratamiento de Datos contempla una excepción análoga.
- 25 A continuación, el órgano jurisdiccional remitente se refiere, en particular, al artículo 52, apartado 1, de la Carta, que establece el principio según el cual debe existir una relación de proporcionalidad entre el objetivo perseguido por la injerencia en los derechos y libertades de los ciudadanos y los medios utilizados.
- 26 Ahora bien, según dicho órgano jurisdiccional, el sistema de videovigilancia controvertido no parece haber sido utilizado de una manera o con una finalidad que no se corresponda con el objetivo declarado por la comunidad de propietarios, a saber, proteger la vida, la integridad física y la salud de los interesados, esto es, de los copropietarios del edificio en el que se instaló el sistema.

- 27 Dadas estas circunstancias, el Tribunalul București (Tribunal de Distrito de Bucarest, Rumanía) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:
- «1) ¿Deben interpretarse los artículos 8 y 52 de la Carta, así como el artículo 7, letra f), de la Directiva 46/95 en el sentido de que se oponen a disposiciones nacionales como las controvertidas en el litigio principal, esto es, el artículo 5, apartado 2, de la [Ley n.º 677/2001] y el artículo 6 de la Decisión de la Autoridad de Supervisión del Tratamiento de Datos n.º 52/2012, que establece la posibilidad de videovigilancia para garantizar el cuidado y la protección de las personas, bienes y activos y para satisfacer intereses legítimos, sin el consentimiento del interesado?
 - 2) ¿Deben interpretarse los artículos 8 y 52 de la Carta en el sentido de que la restricción de los derechos y libertades mediante videovigilancia respeta el principio de proporcionalidad y las exigencias de que “[sea necesaria]” y de que “[responda] efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás” cuando el responsable del tratamiento tiene la posibilidad de adoptar otras medidas para proteger el interés legítimo de que se trata?
 - 3) ¿Debe interpretarse el artículo 7, letra f), de la Directiva 46/95, en el sentido de que el “interés legítimo” del responsable de tratamiento debe probarse, así como existir y ser actual en relación con el momento del tratamiento?
 - 4) ¿Debe interpretarse el artículo 6, apartado 1, letra e), de la Directiva 46/95, en el sentido de que un tratamiento (videovigilancia) es excesivo o no es adecuado cuando el responsable del tratamiento tiene la posibilidad de adoptar otras medidas para proteger el interés legítimo de que se trata?»

Acerca de las cuestiones prejudiciales

- 28 Con carácter preliminar, procede en primer lugar señalar que, aunque el órgano jurisdiccional remitente se refiere, en su cuarta cuestión prejudicial, al artículo 6, apartado 1, letra e), de la Directiva 95/46, no aporta ninguna explicación sobre la pertinencia de esta disposición para la resolución del litigio principal.
- 29 En efecto, esta disposición trata únicamente sobre las exigencias a las que debe responder la conservación de datos personales. Sin embargo, nada en los autos ante el Tribunal de Justicia permite suponer que el litigio principal verse sobre este aspecto.
- 30 En cambio, procede señalar que, en la medida en que el órgano jurisdiccional remitente pregunta, en esencia, en dicha cuestión prejudicial, si el establecimiento de un sistema de videovigilancia como el controvertido en el litigio principal es proporcionado a los fines perseguidos, la cuestión de si los datos personales recogidos por dicho sistema cumplen la exigencia de proporcionalidad se refiere a la interpretación del artículo 6, apartado 1, letra c), de la Directiva 95/46.
- 31 Esta última disposición debe tenerse en cuenta a la hora de comprobar si concurre el segundo requisito de aplicación impuesto en el artículo 7, letra f), de la Directiva 95/46, según el cual el tratamiento de los datos personales debe ser «necesario» para la satisfacción del interés legítimo perseguido.
- 32 En segundo lugar, mediante sus cuestiones prejudiciales primera y segunda, el órgano jurisdiccional remitente se refiere a los artículos 8 y 52 de la Carta, tomados de manera aislada o en combinación con el artículo 7, letra f), de la Directiva 95/46. Ahora bien, el Tribunal de Justicia ya ha precisado que el requisito impuesto en esta disposición, en relación con la existencia de derechos y libertades fundamentales del interesado en la protección de datos que prevalezcan sobre el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, exige que se proceda a una ponderación de los derechos e intereses en conflicto, que dependerá

de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta confieren al interesado (sentencia de 24 de noviembre de 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 y C-469/10, EU:C:2011:777, apartado 40). De ello se deduce que, en este caso, tales artículos 8 y 52 no deben aplicarse de forma aislada.

- 33 Habida cuenta de lo anterior, procede considerar que, mediante sus cuestiones prejudiciales, que deben examinarse conjuntamente, el órgano jurisdiccional remitente pregunta, en esencia, si los artículos 6, apartado 1, letra c), y 7, letra f), de la Directiva 95/46, a la luz de los artículos 7 y 8 de la Carta, deben interpretarse en el sentido de que se oponen a disposiciones nacionales que permiten la instalación de un sistema de videovigilancia como el controvertido en el litigio principal, colocado en las zonas comunes de un edificio de uso residencial con el fin de satisfacer intereses legítimos consistentes en garantizar el cuidado y la protección de las personas y de los bienes, sin el consentimiento de los interesados.
- 34 Debe recordarse que una vigilancia efectuada mediante la grabación en vídeo de imágenes de personas que se almacenan en un dispositivo de grabación continuada, a saber, el disco duro, constituye, conforme al artículo 3, apartado 1, de la Directiva 95/46, un tratamiento automatizado de datos personales (sentencia de 11 de diciembre de 2014, Ryněš, C-212/13, EU:C:2014:2428, apartado 25).
- 35 Por consiguiente, un sistema de videovigilancia mediante cámaras debe calificarse de tratamiento automatizado de datos personales en el sentido de dicha disposición cuando el dispositivo instalado permita grabar y almacenar datos personales, como imágenes con las que pueda identificarse a personas físicas. Corresponde al órgano jurisdiccional remitente comprobar si el sistema controvertido en el litigio principal presenta tales características.
- 36 Además, todo tratamiento de datos personales debe, por una parte, ser conforme con los principios relativos a la calidad de los datos, enunciados en el artículo 6 de la Directiva 95/46, y, por otra, responder a alguno de los principios relativos a la legitimación del tratamiento de datos, enumerados en el artículo 7 de dicha Directiva (sentencia de 13 de mayo de 2014, Google Spain y Google, C-131/12, EU:C:2014:317, apartado 71 y jurisprudencia citada).
- 37 El artículo 7 de la Directiva 95/46 prevé una lista exhaustiva y taxativa de los casos en los que un tratamiento de datos personales puede considerarse lícito. Los Estados miembros no pueden añadir a dicho artículo nuevos principios relativos a la legitimación de los tratamientos de datos personales ni imponer exigencias adicionales que vendrían a modificar el alcance de alguno de los seis principios establecidos en dicho artículo (sentencia de 19 de octubre de 2016, Breyer, C-582/14, EU:C:2016:779, apartado 57).
- 38 De ello se deduce que, para poder ser considerado legítimo, el tratamiento de datos personales debe estar comprendido en uno de los seis casos contemplados en el artículo 7 de la Directiva 95/46.
- 39 Las cuestiones planteadas por el órgano jurisdiccional remitente se refieren, en particular, al principio de legitimación de las operaciones de tratamiento de datos contemplado en el artículo 7, letra f), de la Directiva 95/46, disposición que fue traspuesta al ordenamiento jurídico rumano mediante el artículo 5, apartado 2, letra e), de la Ley n.º 677/2001, al que también remite el artículo 6 de la Decisión n.º 52/2012 de la Autoridad de Supervisión del Tratamiento de Datos en lo que atañe específicamente al tratamiento de datos personales mediante la videovigilancia.
- 40 A este respecto, el artículo 7, letra f), de la Directiva 95/46 fija tres requisitos acumulativos para que el tratamiento de datos personales resulte lícito: primero, que el responsable del tratamiento o el tercero o terceros a quienes se comuniquen los datos persigan un interés legítimo; segundo, que el tratamiento de datos personales sea necesario para la satisfacción de ese interés legítimo; y, tercero, que no

prevalezcan sobre el interés legítimo perseguido los derechos y libertades fundamentales del interesado en la protección de los datos (sentencia de 4 de mayo de 2017, *Rigas satiksme*, C-13/16, EU:C:2017:336, apartado 28).

- 41 Procede subrayar que el artículo 7, letra f), de la Directiva 95/46 no requiere el consentimiento de la persona interesada. Sin embargo, tal consentimiento únicamente figura en el artículo 7, letra a), de dicha Directiva como requisito al que está supeditado el tratamiento de datos personales.
- 42 En el caso de autos, el objetivo que persigue, en esencia, el responsable del tratamiento de los datos cuando instala un sistema de videovigilancia como el controvertido en el litigio principal, a saber, la protección de los bienes, de la salud y de la vida de los copropietarios de un inmueble, puede calificarse de «interés legítimo» en el sentido del artículo 7, letra f), de la Directiva 95/46. Por lo tanto, el primer requisito fijado en esa disposición parece concurrir (véase, por analogía, la sentencia de 11 de diciembre de 2014, *Ryneš*, C-212/13, EU:C:2014:2428, apartado 34).
- 43 No obstante, el órgano jurisdiccional remitente se pregunta si el primero de los requisitos establecidos en el artículo 7, letra f), debe entenderse en el sentido de que el interés perseguido por el responsable en cuestión debe, por una parte, «probarse» y, por otra, «existir y ser actual en relación con el momento del tratamiento».
- 44 A este respecto, procede señalar que, tal como han alegado los Gobiernos rumano y checo, Irlanda, el Gobierno austriaco, el Gobierno portugués y la Comisión, toda vez que, de conformidad con el artículo 7, letra f), de la Directiva 95/46, el responsable del tratamiento de datos personales o el tercero a quien se comuniquen los datos debe perseguir un interés legítimo que justifique ese tratamiento, dicho interés debe existir y ser actual en la fecha del tratamiento y no tener carácter hipotético en esa fecha. Sin embargo, a la hora de apreciar todas las circunstancias del caso no puede exigirse necesariamente que haya habido anteriormente un perjuicio para la seguridad de los bienes y de las personas.
- 45 En el caso de autos parece concurrir en todo caso, en una situación como la del litigio principal, el requisito relativo a la existencia de un interés y a la actualidad del mismo, puesto que el órgano jurisdiccional remitente señala que los allanamientos, los robos y los actos de vandalismo se produjeron antes de que se instalara el sistema de videovigilancia y pese a la instalación, en la entrada del edificio, de un sistema de seguridad compuesto por un interfono y una tarjeta magnética.
- 46 Por lo que se refiere al segundo requisito impuesto en el artículo 7, letra f), de la Directiva 95/46, basado en la necesidad de recurrir al tratamiento de datos personales para satisfacer el interés legítimo perseguido, el Tribunal de Justicia ha recordado que las excepciones y restricciones al principio de protección de los datos de carácter personal deben establecerse sin sobrepasar los límites de lo estrictamente necesario (sentencia de 4 de mayo de 2017, *Rigas satiksme*, C-13/16, EU:C:2017:336, apartado 30 y jurisprudencia citada).
- 47 Este requisito exige que el órgano jurisdiccional remitente compruebe que el interés legítimo del tratamiento de datos, perseguido por la videovigilancia controvertida en el litigio principal y consistente, en esencia, en garantizar la seguridad de los bienes y de las personas y en prevenir la comisión de delitos, no puede alcanzarse razonablemente de manera tan eficaz por otros medios menos atentatorios respecto de los derechos y libertades fundamentales de los interesados, en particular respecto de los derechos al respeto de la vida privada y de protección de los datos personales, garantizados por los artículos 7 y 8 de la Carta.

- 48 Además, tal como alegó la Comisión, el requisito relativo a la necesidad del tratamiento debe examinarse en relación con el llamado principio de «minimización de los datos», consagrado en el artículo 6, apartado 1, letra c), de la Directiva 95/46, conforme al cual los datos personales deben ser «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente».
- 49 De los autos ante el Tribunal de Justicia resulta que la exigencia de proporcionalidad parece haberse tenido en cuenta en el tratamiento de datos de que se trata en el litigio principal. Consta, en efecto, que inicialmente se adoptaron medidas alternativas, consistentes en un sistema de seguridad instalado en la entrada del edificio y compuesto por un interfono y una tarjeta magnética, pero que resultaron insuficientes. Además, el sistema de videovigilancia en cuestión se limita a las zonas comunes de la copropiedad y a las vías de acceso a la misma.
- 50 Sin embargo, la proporcionalidad del tratamiento de los datos mediante un sistema de videovigilancia debe apreciarse teniendo en cuenta el modo concreto de instalación y de funcionamiento de dicho dispositivo, que debe limitar el impacto del mismo en los derechos y libertades de los interesados a la vez que garantizar la eficacia del sistema de videovigilancia de que se trate.
- 51 De este modo, como ha alegado la Comisión, el requisito relativo a la necesidad del tratamiento implica que el responsable del tratamiento debe examinar, por ejemplo, si basta con que la videovigilancia solo funcione de noche o fuera de las horas normales de trabajo, y bloquear o difuminar las imágenes tomadas en las zonas que no sea necesario vigilar.
- 52 Por último, en relación con el tercer requisito impuesto en el artículo 7, letra f), de la Directiva 95/46, en relación con la existencia de derechos y libertades fundamentales del interesado en la protección de los datos que prevalezcan sobre el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, procede recordar, como ya se ha mencionado en el apartado 32 de la presente sentencia, que la apreciación de este requisito requiere proceder a una ponderación de los derechos e intereses en conflicto a la luz de las circunstancias específicas del caso, en el marco de la cual deberá tenerse en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta confieren al interesado.
- 53 En este contexto, el Tribunal de Justicia ha declarado que el artículo 7, letra f), de la Directiva 95/46 se opone a que un Estado miembro excluya de manera categórica y generalizada la posibilidad de someter a tratamiento determinadas categorías de datos personales, sin permitir una ponderación de los derechos e intereses en conflicto en cada caso concreto. Un Estado miembro no puede establecer con carácter definitivo el resultado de la ponderación de los derechos e intereses en conflicto respecto de tales categorías sin permitir un resultado diferente en atención a las circunstancias particulares de cada caso concreto (sentencia de 19 de octubre de 2016, Breyer, C-582/14, EU:C:2016:779, apartado 62).
- 54 De la jurisprudencia del Tribunal de Justicia también se desprende que cabe tomar en consideración, a efectos de esta ponderación, el hecho de que la gravedad de la lesión de los derechos fundamentales de la persona afectada por el tratamiento en cuestión puede variar en función de si es posible acceder a los datos de que se trate a través de fuentes ya disponibles para el público (véase, en este sentido, la sentencia de 4 de mayo de 2017, Rigas satiksme, C-13/16, EU:C:2017:336, apartado 32).
- 55 A diferencia de los tratamientos de datos que figuran en fuentes accesibles al público, los tratamientos de datos que figuran en fuentes no accesibles al público implican que el responsable del tratamiento y, en su caso, el tercero o terceros a quienes se comuniquen los datos dispondrán en lo sucesivo de ciertas informaciones sobre la vida privada del interesado. Esta lesión, más grave, de los derechos del interesado consagrados en los artículos 7 y 8 de la Carta debe ser apreciada en su justo valor, contrapesándola con el interés legítimo perseguido por el responsable del tratamiento o por el tercero

o terceros a los que se comuniquen los datos (véase, en este sentido, la sentencia de 24 de noviembre de 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 y C-469/10, EU:C:2011:777, apartado 45).

- 56 El criterio relativo a la gravedad de la lesión de los derechos y libertades del interesado constituye un elemento esencial del ejercicio de ponderación, o de ponderación caso por caso, exigido por el artículo 7, letra f), de la Directiva 95/46.
- 57 A este respecto, debe tenerse en cuenta, en particular, la naturaleza de los datos personales en cuestión, en particular el carácter potencialmente sensible de los mismos, así como la naturaleza y el modo concreto del tratamiento de los datos de que se trata, en particular el número de personas que tienen acceso a ellos y el modo en que acceden.
- 58 También son pertinentes, a efectos de esta ponderación, las expectativas razonables del interesado de que sus datos personales no sean objeto de tratamiento cuando, en las circunstancias del caso, esa persona no pudiera esperar razonablemente un tratamiento posterior de los mismos.
- 59 Por último, tales elementos deben sopesarse en relación con la importancia, para todos los copropietarios del edificio, del interés legítimo perseguido en este caso por el sistema de videovigilancia de que se trata, en la medida en que pretende esencialmente garantizar la protección de la propiedad, de la salud y de la vida de dichos copropietarios.
- 60 Habida cuenta de las consideraciones anteriores, procede responder a las cuestiones prejudiciales planteadas que los artículos 6, apartado 1, letra c), y 7, letra f), de la Directiva 95/46, deben interpretarse, a la luz de los artículos 7 y 8 de la Carta, en el sentido de que no se oponen a disposiciones nacionales que autorizan la instalación de un sistema de videovigilancia como el controvertido en el litigio principal, colocado en las zonas comunes de un edificio de uso residencial sin el consentimiento de los interesados, con el fin de satisfacer intereses legítimos consistentes en garantizar el cuidado y la protección de las personas y de los bienes, si el tratamiento de datos personales mediante el sistema de videovigilancia de que se trata reúne los requisitos impuestos en dicho artículo 7, letra f), circunstancia que corresponde verificar al órgano jurisdiccional remitente.

Costas

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

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

Los artículos 6, apartado 1, letra c), y 7, letra f), de 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, deben interpretarse, a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, en el sentido de que no se oponen a disposiciones nacionales que autorizan la instalación de un sistema de videovigilancia como el controvertido en el litigio principal, colocado en las zonas comunes de un edificio de uso residencial sin el consentimiento de los interesados, con el fin de satisfacer intereses legítimos consistentes en garantizar el cuidado y la protección de las personas y de los bienes, si el tratamiento de datos personales mediante el sistema de videovigilancia de que se trata reúne los requisitos impuestos en dicho artículo 7, letra f), circunstancia que corresponde verificar al órgano jurisdiccional remitente.

Firmas