Asunto C-793/19

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:

29 de octubre de 2019

Órgano jurisdiccional remitente:

Bundesverwaltungsgericht (Tribunal Supremo de lo Contencioso-Administrativo, Alemania)

Fecha de la resolución de remisión:

25 de septiembre de 2019

Parte demandante y recurrida en casación:

SpaceNet AG

Parte demandada y recurrente en casación:

Bundesrepublik Deutschland (República Federal de Alemania)

Objeto del procedimiento principal

Demanda con el objeto de que se declare que SpaceNet no está obligada a almacenar los datos sobre tráfico de telecomunicaciones mencionados en el artículo 113b, apartado 3, de la TKG, de los clientes a los que proporciona acceso a Internet.

Objeto y fundamento jurídico de la petición de decisión prejudicial

Interpretación del Derecho de la Unión, en particular del artículo 15, apartado 1, de la Directiva 2002/58 y de la sentencia Tele2 Sverige y Watson y otros; artículo 267 TFUE.

Cuestión prejudicial

«¿Debe interpretarse el artículo 15 de la Directiva 2002/58/CE, a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de

la Unión Europea, por un lado, y del artículo 6 de la Carta de los Derechos Fundamentales de la Unión Europea y del artículo 4 del Tratado de la Unión Europea, por otro, en el sentido de que se opone a una normativa nacional que obliga a los proveedores de servicios de comunicaciones electrónicas disponibles al público a conservar los datos de tráfico y de localización de los usuarios finales de dichos servicios, cuando:

– la obligación en cuestión no está sujeta a ninguna condición específica, ya sea geográfica, temporal o espacial;

– en el caso de prestación de servicios de telefonía disponibles al público (incluida la transmisión de mensajes breves, multimedia o similares y de llamadas perdidas o no respondidas), la obligación en cuestión tiene por objeto los siguientes datos:

  – el número de teléfono u otra identificación de la línea de origen y de destino y, en caso de redirección o desvió de llamada, de las demás líneas intervinientes;

  – la fecha y hora de inicio y fin de la comunicación o, en caso de transmisión de mensajes breves, multimedia o similares, la hora de envío y recepción del mensaje, con indicación de la zona horaria;

  – datos del servicio utilizado, en caso de que en el marco del servicio telefónico puedan utilizarse distintos servicios;

  – en caso de servicios de telefonía móvil, además:

    – la identificación internacional del usuario móvil para la línea de origen y de destino;

    – la identificación internacional del terminal de origen y de destino;

    – la fecha y hora de la primera activación del servicio, con indicación de la zona horaria, en caso de servicios de pago anticipado;

    – denominación de las células utilizadas al inicio de la comunicación por la línea de origen y de destino;

  – en caso de servicios de telefonía por Internet, además, las direcciones de protocolo de Internet de la línea de origen y de destino y las identificaciones de usuario asignadas;

– en el caso de prestación de servicios de acceso a Internet disponibles al público, la obligación de almacenamiento tiene por objeto los siguientes datos:

  - la dirección de protocolo de Internet asignada al usuario para cada uso de Internet;
  - una identificación exclusiva de la línea utilizada para el uso de Internet, y la identificación de usuario asignada;
  - la fecha y hora de inicio y fin del uso de Internet con la dirección de protocolo de Internet asignada, con indicación de la zona horaria;
  - en caso de uso móvil, la denominación de la célula utilizada al inicio de la conexión;
- no se permite almacenar los siguientes datos:
  - el contenido de la comunicación;
  - datos de los sitios web visitados;
  - datos de los servicios de correo electrónico;
  - datos relativos a comunicaciones a o desde determinadas líneas de personas, autoridades u organizaciones de ámbitos sociales o religiosos;
- el plazo de conservación de los datos de localización, es decir, la denominación de la célula utilizada, es de cuatro semanas; para los demás datos, el plazo es de diez semanas;
- se garantiza una protección efectiva de los datos almacenados frente a cualquier uso indebido y frente a cualquier acceso no autorizado, y
- solo se permite la utilización de los datos almacenados con fines de investigación de delitos graves y para la prevención de un riesgo concreto para la vida, la integridad física o la libertad de las personas o para la seguridad de la Federación o de un Land, con excepción de la dirección de protocolo de Internet asignada al usuario para cada uso de Internet, cuya utilización se autoriza en el marco de transmisiones de extractos de la base de datos con fines de investigación de cualquier tipo de delito y para prevenir riesgos para la seguridad pública y el orden público y no obstaculizar las funciones de los servicios de inteligencia?»

Disposiciones del Derecho de la Unión invocadas

Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), artículos 6, 7, 8, 11 y 52

Tratado de la Unión Europea (en lo sucesivo, «TUE»): artículos 4 y 6

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE, del Parlamento Europea y del Consejo, de 25 de noviembre de 2009 (en lo sucesivo, Directiva 2002/58), artículos 5, 6, 8 y 9 y, en particular, el artículo 15 y el considerando 11.

Disposiciones de Derecho nacional invocadas

Telekommunikationsgesetz (Ley de telecomunicaciones; en lo sucesivo, «TKG»), artículo 113a, apartado 1, primera frase («Obligados»); artículo 113b («Obligaciones de almacenamiento de datos de tráfico»); artículo 113c («Uso de los datos»); artículo 113d («Protección de los datos»); artículo 113e [«Protocolización» [por el obligado, respecto de los accesos a los datos almacenados)]; artículo 113f [«Catálogo de requisitos» (relativos a las precauciones técnicas y demás medidas)], y artículo 99, apartado 2 («Facturación detallada», organismos que no han de aparecer en la factura detallada)

Strafprozessordnung (Ley de enjuiciamiento criminal; en lo sucesivo, «StPO»): artículo 100g, apartado 2 («Recogida de datos de tráfico» con arreglo al artículo 113b de la TKG)

Jurisprudencia del Tribunal de Justicia citada

Sentencia del Tribunal de Justicia de la Unión Europea de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970; en lo sucesivo, «sentencia Tele2 Sverige y Watson y otros»)

Sentencia de 8 de abril de 2014, Digital Rights Ireland y Seitlinger y otros (C-293/12 y C-594/12, EU:C:2014:238; en lo sucesivo, «sentencia Digital Rights Ireland y otros»)

Dictamen 1/15 de 26 de julio de 2017, EU:C:2017:592

Asimismo, sentencias de 29 de julio de 2019, Funke Medien (C-469/17, EU:C:2019:623); de 9 de marzo de 1978, Simmenthal (106/77, EU:C:1978:49); de 3 de mayo de 2005, Berlusconi y otros (C-387/02, C-391/02 y C-403/02, EU:C:2005:270); de 22 de junio de 2010, Melki y Abdeli (C-188/10 y C-189/10, EU:C:2010:363), y de 18 de septiembre de 2014, Vueling Airlines (C-487/12, EU:C:2014:2232).

Breve exposición de los hechos y del procedimiento principal

1 La demandante, SpaceNetAG (en lo sucesivo, «demandante» o «SpaceNet»), se dedica a la prestación de servicios de acceso a Internet disponibles al público. Se

opone a la obligación que le impone el artículo 113a, apartado 1, en relación con el artículo 113b de la TKG en su versión resultante de la Ley de 10 de diciembre de 2015, de almacenar los datos de tráfico de telecomunicaciones de sus clientes a partir del 1 de julio de 2017.

2 En primera instancia, el Verwaltungsgericht (Tribunal de lo Contencioso-Administrativo) declaró que SpaceNet no está obligada a almacenar los datos de tráfico de telecomunicaciones mencionados en el artículo 113b, apartado 3, de la TKG relativos a los clientes a los que proporciona acceso a Internet. Contra la sentencia de dicho Tribunal, la República Federal de Alemania (en lo sucesivo, «demandada») ha interpuesto recurso de casación directo.

3 El recurso de casación habrá de prosperar si la obligación de almacenar los datos de tráfico de telecomunicaciones que se impone a los proveedores de servicios de comunicaciones electrónicas disponibles al público (en lo sucesivo, «proveedores de telecomunicaciones»), en virtud de las citadas disposiciones de la TKG, no es contraria al Derecho de la Unión.

4 La regulación de esta obligación de los proveedores de telecomunicaciones de almacenar datos durante un cierto período de tiempo ha sido modificada por la Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Ley de introducción de una obligación y un plazo máximo de almacenamiento de datos de tráfico) de 10 de diciembre de 2015 (en lo sucesivo, «Ley de 10 de diciembre de 2015»).

5 Era necesaria una nueva regulación tras la sentencia del Bundesverfassungsgericht (Tribunal Constitucional Federal, Alemania) de 2010 en la que se declararon nulas las disposiciones anteriores relativas a la conservación de datos, por vulneración de derechos fundamentales, así como tras la sentencia Digital Rights Ireland y otros, de 2014, en la que fue declarada nula la Directiva 2006/24, para cuya transposición se habían adoptado aquellas disposiciones. La Ley de 10 de diciembre de 2015 pretende suplir el vacío normativo resultante en materia de persecución de delitos y de prevención de riesgos y, al mismo tiempo, tomar en consideración las mencionadas resoluciones judiciales de las instancias constitucional y europea.

6 Para responder a la cuestión prejudicial relativa a la compatibilidad con el Derecho de la Unión de la obligación de almacenamiento que impone el artículo 113a, apartado 1, en relación con el artículo 113b, de la TKG, es necesaria una interpretación de la Directiva 2002/58 por parte del Tribunal de Justicia; en particular, se precisa una aclaración sobre cómo se ha de entender la sentencia Tele2 Sverige y Watson y otros.

Breve exposición de la fundamentación de la petición de decisión prejudicial

7 La obligación de almacenamiento de los datos de tráfico de telecomunicaciones que establece el artículo 113a, apartado 1, primera frase, en relación con el

artículo 113b, de la TKG restringe los derechos que se derivan de los artículos 5, apartado 1; 6, apartado 1, y 9, apartado 1, de la Directiva 2002/58.

8 Constituye una injerencia en la confidencialidad de las comunicaciones electrónicas, consagrada en el artículo 5, apartado 1, primera frase, de la Directiva, y vulnera el principio que prohíbe a toda persona distinta del usuario almacenar, sin el consentimiento de este, los datos de tráfico relativos a comunicaciones electrónicas.

9 Asimismo, incumple el precepto del artículo 6 de la Directiva, conforme al cual los datos de tráfico solo deben ser tratados y almacenados a efectos de la facturación de los servicios, para su promoción comercial o para la prestación de servicios con valor añadido, y en la medida y durante el tiempo necesario para ello.

10 En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, el artículo 9, apartado 1, primera frase, de la Directiva 2002/58 dispone que solo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido. También se aparta de esta disposición la normativa nacional, en el sentido de que el artículo 113b, apartado 1, punto 2, en relación con el apartado 4, de la TKG también exige el almacenamiento de los datos de localización a los que hace referencia.

11 La restricción de los derechos que confieren los artículos 5, apartado 1; 6, apartado 1, y 9, apartado 1, de la Directiva 2002/58 solo estará justificada si la disposición del artículo 113a, apartado 1, primera frase, en relación con el artículo 113b, de la TKG puede ampararse en el artículo 15, apartado 1, de la Directiva 2002/58.

12 Conforme a este último, los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5, 6, 8, apartados 1 a 4, y 9 de la misma Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el artículo 13, apartado 1, de la Directiva 95/46. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el apartado citado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en el artículo 6, apartados 1 y 2, del Tratado de la Unión Europea (TUE).

13 Conforme a las consideraciones formuladas por el Tribunal de Justicia en la sentencia Tele2 Sverige y Watson y otros, en particular en sus apartados 82 y siguientes y 108 y siguientes, para que una norma nacional sobre conservación de datos sea válida, el artículo 15, apartado 1, de la Directiva 2002/58 exige que exista una razón suficiente. Esto significa que solo afecta a las personas sobre las que pesen indicios de una relación con graves delitos, que la obligación se limite a la región, el período y a los medios de comunicación pertinentes al respecto, y que solo se deben recoger los datos que sean indispensables para el esclarecimiento de los delitos de que se trate.

14 Obviamente, la posición de la demandada es opuesta a estos principios, al entender que el solo hecho de que se utilicen servicios de acceso a Internet o de telefonía constituye razón suficiente para el almacenamiento. La apreciación de una incompatibilidad general con el Derecho de la Unión de toda conservación de datos sin motivo, expresada en la sentencia Tele2 Sverige y Watson y otros, no queda desvirtuada tampoco por la referencia que hace la demandada al dictamen del Tribunal de Justicia de 26 de julio de 2017 en relación con el Acuerdo entre Canadá y la Unión Europea sobre la transferencia de los datos de los pasajeros aéreos. Es cierto que el Tribunal de Justicia, en cuanto a la necesidad de la injerencia que implica el Acuerdo en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, ha subrayado que los datos PNR se transmiten a Canadá con independencia de si existen o no indicios objetivos de que los pasajeros constituyan un peligro para la seguridad pública en Canadá. Sin embargo, no se trata en este caso de una conservación de datos sin motivo, ya que el almacenamiento y tratamiento de los datos está relacionado con los controles de frontera, a los cuales están sometidos todos los pasajeros aéreos que deseen entrar o salir de Canadá, con arreglo a la legislación canadiense. Al abandonar el país, desaparece el motivo para el almacenamiento, de modo que, a partir de ese momento, la necesidad de una nueva razón conduce a que la conservación presuponga la existencia de indicios objetivos de que los pasajeros de que se trate podrían constituir un peligro en relación con la lucha contra el terrorismo y la delincuencia internacional grave.

15 Si debe entenderse la jurisprudencia del Tribunal de Justicia en el sentido de que la conservación de los datos sin una razón no es en ningún caso compatible con el Derecho de la Unión, el recurso de casación que la demandada ha interpuesto contra la sentencia del Verwaltungsgericht no puede prosperar. En efecto, al igual que sucede con las normativas sueca y británica sobre conservación de datos, que fueron objeto de la sentencia Tele2 Sverige y Watson y otros, el artículo 113a, apartado 1, primera frase, en relación con el artículo 113b, de la TKG no exige ni la existencia de un motivo suficiente (más allá de la mera utilización de los servicios de acceso a Internet o telefónicos) para el almacenamiento, ni una relación entre los datos almacenados y un hecho delictivo o un peligro para la seguridad pública. Dicha disposición prescribe más bien el almacenamiento de gran parte de los datos de tráfico de telecomunicaciones relevantes, sin ninguna razón, en todo el territorio y sin distinción personal, temporal y geográfica.

16 No obstante, al margen de las consideraciones formuladas en la sentencia Tele2 Sverige y Watson y otros, el órgano jurisdiccional remitente no excluye que la obligación de conservación de datos de tráfico de telecomunicaciones sin motivo que establece el artículo 113a, apartado 1, primera frase, en relación con el artículo 113b, de la TKG pueda fundamentarse en el artículo 15, apartado 1, de la Directiva 2002/58, por las siguientes razones:

17 En primer lugar, las disposiciones controvertidas de la TKG no exigen el almacenamiento de todos los datos de tráfico de telecomunicaciones de todos los usuarios y abonados en relación con todos los medios de comunicación electrónicos. De la obligación de conservación están excluidos no solo el contenido de la comunicación, sino también los datos sobre los sitios web visitados, sobre los servicios de correo electrónico y los relativos a comunicaciones con determinadas líneas de ámbitos sociales o religiosos (véase el artículo 113b, apartados 5 y 6, de la TKG). Si determinados medios de comunicación o determinados tipos de datos quedan excluidos de la obligación de almacenamiento, puede reducirse considerablemente el riesgo de elaboración de un perfil completo de las personas, aunque no se elimine del todo.

18 En segundo lugar, el órgano jurisdiccional remitente entiende que otra diferencia aún más importante entre la normativa controvertida de la TKG en el caso de autos, de un lado, y la anterior regulación de la Directiva 2006/24, y las legislaciones sueca y británica basadas en ella y que fueron objeto de la sentencia Tele2 Sverige y Watson y otros, de otro, reside en que el plazo de almacenamiento se ha visto sustancialmente reducido por el artículo 113b, apartado 1, de la TKG, pasando de seis meses a dos años (véase el artículo 6 de la Directiva 2006/24) a de cuatro a diez semanas.

19 El riesgo de elaboración de un perfil completo del interesado resulta menor cuanto más reducido es el período en el que se hallan almacenados los datos de tráfico. Cuanto menor es dicho período, más incompleto es necesariamente el perfil de personalidad y menos intensa la incidencia en los derechos fundamentales.

20 En tercer lugar, las disposiciones de la TKG controvertidas en el caso de autos están sujetas a estrictas limitaciones en cuanto a la protección de los datos almacenados y el acceso a tales datos. Por un lado, las disposiciones de los artículos 113d y siguientes de la TKG ofrecen una protección efectiva de los datos almacenados frente al riesgo de un uso indebido y un acceso no autorizado. Por otro, de conformidad con el artículo 113c, apartado 1, de la TKG, los datos almacenados solo pueden utilizarse para combatir graves delitos o para prevenir riesgos concretos para la vida, la integridad física o la libertad de las personas o para la seguridad del Estado o de un Land.

21 La recogida de datos de tráfico con fines de persecución de los delitos presupone, con arreglo al artículo 100g, apartado 2, de la StPO, que existe la sospecha de un delito claramente tipificado en la ley como especialmente grave, que se trata además de un hecho de especial gravedad, que la investigación de los hechos o la

averiguación del paradero del sospechoso por otros medios resulta sustancialmente más complicada o inviable y que la recogida de los datos es proporcionada con respecto a la importancia del caso. El artículo 100g, apartado 4, de la StPO no permite la recogida o utilización de datos de tráfico de las personas sujetas a secreto profesional con arreglo al artículo 53, apartado 1, primera frase, puntos 1 a 5, de la StPO, entre las que se incluyen, por ejemplo, los abogados, los médicos o los periodistas. Además, el artículo 101a, apartado 1, de la StPO somete a autorización judicial la recogida de los datos de tráfico a que se refiere el artículo 100g de la citada Ley.

22 Es cierto que este régimen de acceso restringido no se aplica a la dirección de protocolo de Internet asignada al usuario para cada uso de Internet, pues, con arreglo al artículo 113c, apartado 1, punto 3, de la TKG, estos datos se pueden utilizar también dentro de transmisiones de extractos de la base de datos con el fin de investigar cualquier tipo de delito, prevenir riesgos para la seguridad pública y el orden público y cumplir las funciones de los servicios de inteligencia. No obstante, se ha de recordar que la información acerca del titular de la línea que está registrado en Internet en una dirección de protocolo ya conocida no permite la elaboración de perfiles de personalidad y de movimientos.

23 Aun dando por válida la argumentación de SpaceNet y admitiendo que cada vez se utilicen en mayor medida procedimientos técnicos con los que las direcciones de protocolo de Internet ya no puedan atribuirse claramente a una determinada línea de telecomunicaciones, sino solo un grupo más amplio de líneas, de manera que los extractos de bases de datos se han convertido en una medida ampliamente difundida, la incidencia de estos extractos sigue siendo de mucho menor intensidad que la que se produce con la recogida y utilización de los propios datos de tráfico de telecomunicaciones.

24 En cuarto lugar, en pro de la posibilidad de que el artículo 15, apartado 1, de la Directiva 2002/58 justifique la obligación de almacenar los datos de tráfico de telecomunicaciones establecida en el artículo 113a, apartado 1, primera frase, en relación con el artículo 113b, de la TKG podría argumentarse que el legislador no ha hecho sino cumplir con los deberes de actuación que implica para los Estados miembros el derecho a la seguridad consagrado en el artículo 6 de la Carta. En la sentencia Digital Rights Ireland y otros, el Tribunal de Justicia mencionó expresamente esta disposición y, a este respecto, declaró que la lucha contra el terrorismo internacional para el mantenimiento de la paz y la seguridad internacionales es un objetivo de interés general de la Unión, y que lo mismo ocurre en cuanto a la lucha contra la delincuencia grave en defensa de la seguridad pública.

25 En estas circunstancias, el órgano jurisdiccional remitente alberga dudas acerca de si la jurisprudencia del Tribunal de Justicia debe interpretarse en el sentido de que el almacenamiento de datos sin motivo no solo es ilícita en la forma concreta en que se reguló en la Directiva 2006/24 y en las legislaciones sueca y británica basadas en esta, sino que, con carácter general, no puede ampararse en el artículo

15, apartado 1, de la Directiva 2002/58. En efecto, el concepto básico de almacenamiento de datos es incompatible con la exigencia, formulada con carácter absoluto por el Tribunal de Justicia, de diferenciar, respecto a los datos en cuestión, en función de las personas, los períodos de tiempo y las áreas geográficas.

26 En contra de la tesis de que el almacenamiento sin motivo de los datos de tráfico es, de por sí, incompatible con la Carta, puede aducirse, a juicio del órgano jurisdiccional remitente, la necesidad de hallar un equilibrio entre, por un lado, el deber de los Estados miembros de garantizar la seguridad de las personas que residen en su territorio, y por otro, el respeto de los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta.

27 Así pues, el órgano jurisdiccional remitente no alcanza a percibir que la jurisprudencia del Tribunal de Justicia, con claridad, cierre el paso a que los legisladores nacionales puedan establecer, tras una adecuada ponderación, un almacenamiento de datos sin motivo (si es preciso, complementada con un estricto régimen de acceso), que tenga en cuenta el riesgo potencial específico que se deriva de los nuevos medios de telecomunicación.

28 En quinto lugar, el órgano jurisdiccional remitente señala que si, con carácter general, el almacenamiento de datos sin motivo no pudiera ampararse en el artículo 15, apartado 1, de la Directiva 2002/58 y, por lo tanto, fuera irrelevante la forma en que se legisle sobre los medios de telecomunicación afectados, los tipos de datos almacenados, la duración del almacenamiento, los requisitos para el acceso a los datos almacenados y la protección frente a los riesgos de uso indebido, el margen de actuación que le queda al legislador nacional en un ámbito relativo a la persecución de los delitos y a la seguridad pública, que, con arreglo al artículo 4 TUE, apartado 2, tercera frase, sigue siendo en todo caso responsabilidad exclusiva de los Estados miembros, se vería mermado sustancialmente.

29 En sexto y último lugar, a la luz de la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos (en lo sucesivo, «TEDH»), el órgano jurisdiccional remitente no tiene claro si las consideraciones del Tribunal de Justicia en la sentencia Tele2 Sverige y Watson y otros deben entenderse como una prohibición, dirigida a los Estados miembros, de introducir una obligación de almacenamiento sin motivo de los datos de tráfico de telecomunicaciones fundándose en el artículo 15, apartado 1, de la Directiva 2002/58.

30 Recientemente, en una sentencia de 19 de junio de 2018, el TEDH declaró que la legislación sueca de vigilancia masiva del tráfico de datos transfronterizo es conforme con el artículo 8 del Convenio Europeo de los Derechos Humanos y de las Libertades Fundamentales (en lo sucesivo, «CEDH»). Consideró que, habida cuenta de las amenazas que actualmente afrontan los Estados, por ejemplo el flagelo del terrorismo mundial y otros delitos graves, como el narcotráfico, la trata de seres humanos, la explotación sexual de los niños y la delincuencia por

Internet, y ante el progreso tecnológico que facilita a los terroristas y criminales evitar ser descubiertos en Internet, y en atención a la imprevisibilidad de los canales de transmisión de datos electrónicos, la decisión de establecer un sistema de vigilancia masiva para detectar amenazas hasta ahora desconocidas para la seguridad nacional está comprendida en el margen de apreciación que asiste al Estado (sentencia del TEDH de 19 de junio de 2018 n.º 35252/08, ECLI:CE:ECHR:2018:0619JUD003525208, Centrum för Rättvisa/Suecia, apartado 112). Cuando el TEDH alude a la imprevisibilidad de los canales de transmisión de datos electrónicos y al progreso tecnológico, que facilita a los terroristas y criminales evitar ser descubiertos en Internet, hace hincapié de forma más acentuada que el Tribunal de Justicia de la Unión Europea en los potenciales riesgos específicos que llevan aparejados los nuevos medios de telecomunicación.

31 El órgano jurisdiccional remitente se remite al considerando 11 de la Directiva 2002/58 y al artículo 52, apartado 3, de la Carta, de los que se deduce la necesidad de conseguir la coherencia entre los derechos consagrados en la Carta y los reconocidos por el CEDH, sin que con ello se vea afectada la autonomía del Derecho de la Unión y del Tribunal de Justicia de la Unión Europea.

32 Por último, el órgano jurisdiccional remitente hace referencia a otros procedimientos prejudiciales pendientes que tratan de la interpretación de la sentencia Tele2 Sverige y Watson y otros, concretamente la cuestión de si esta sentencia permite deducir una prohibición general de almacenamiento de datos sin motivo que no puede ser obviada por consideraciones relativas a la importancia de los riesgos para la seguridad pública que se pretende combatir ni mediante una «compensación» con un régimen de acceso restrictivo y elevados requisitos de seguridad.

33 A este respecto, se mencionan las peticiones de decisión prejudicial del Investigatory Powers Tribunal – London (Tribunal de Investigación de Londres, Reino Unido) (C-623/17), del Conseil d'État (Consejo de Estado, Francia) (C-511/18 y C-512/18) y de la Cour Constitutionnelle (Tribunal Constitucional, Bélgica) (C-520/18).