Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 21 de diciembre de 2016*

«Procedimiento prejudicial — Comunicaciones electrónicas — Tratamiento de datos personales — Confidencialidad de las comunicaciones electrónicas — Protección — Directiva 2002/58/CE — Artículos 5, 6, 9 y 15, apartado 1 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8, 11 y 52, apartado 1 — Legislación nacional — Proveedores de servicios de comunicaciones electrónicas — Obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización — Autoridades nacionales — Acceso a los datos — Falta de control previo por un órgano jurisdiccional o una autoridad administrativa independiente — Compatibilidad con el Derecho de la Unión»

En los asuntos acumulados C-203/15 y C-698/15,

que tienen por objeto sendas peticiones de decisión prejudicial planteadas, con arreglo al artículo 267 TFUE, por el Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo, Suecia) y la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil) (Reino Unido)], mediante resoluciones, respectivamente, de 29 de abril de 2015 y de 9 de diciembre de 2015, recibidas en el Tribunal de Justicia el 4 de mayo de 2015 y el 28 de diciembre de 2015, en los procedimientos entre

Tele2 Sverige AB (C-203/15)

y

Post- och telestyrelsen,

y

Secretary of State for the Home Department (C-698/15)

y

Tom Watson,

Peter Brice,

Geoffrey Lewis,

con intervención de:

Open Rights Group,

* Lenguas de procedimiento: sueco y inglés.

Privacy International,

The Law Society of England and Wales,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. K. Lenaerts, Presidente, el Sr. A. Tizzano, Vicepresidente, la Sra. R. Silva de Lapuerta, los Sres. T. von Danwitz (Ponente), J.L. da Cruz Vilaça, E. Juhász y M. Vilaras, Presidentes de Sala, y los Sres. A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen y C. Lycourgos, Jueces;

Abogado General: Sr. H. Saugmandsgaard Øe;

Secretario: Sra. C. Strömholm, administradora;

vista la decisión del Presidente del Tribunal de Justicia de 1 de febrero de 2016 de tramitar el asunto C-698/15 mediante el procedimiento acelerado de conformidad con el artículo 105, apartado 1, del Reglamento de Procedimiento del Tribunal de Justicia,

habiendo considerado los escritos obrantes en autos y celebrada la vista el 12 de abril de 2016;

consideradas las observaciones presentadas:

— en nombre de Tele2 Sverige AB, por los Sres. M. Johansson y N. Torgerzon, advokater, y por los Sres. E. Lagerlöf y S. Backman;

— en nombre del Sr. Watson, por el Sr. J. Welch y la Sra. E. Norton, solicitors, el Sr. I. Steele, advocate, el Sr. B. Jaffey, barrister, y la Sra. D. Rose, QC;

— en nombre de los Sres. Brice y Lewis, por los Sres. A. Suterwalla y R. de Mello, barristers, R. Drabble, QC, y S. Luke, solicitor;

— en nombre de Open Rights Group y Privacy International, por el Sr. D. Carey, solicitor, y por el Sr. R. Mehta y la Sra. J. Simor, barristers;

— en nombre de The Law Society of England and Wales, por el Sr. T. Hickman, barrister, y por la Sra. N. Turner;

— en nombre del Gobierno sueco, por las Sras. A. Falk, C. Meyer-Seitz, U. Persson y N. Otte Widgren y el Sr. L. Swedenborg, en calidad de agentes;

— en nombre del Gobierno del Reino Unido, por los Sres. S. Brandon y L. Christie y por la Sra. V. Kaye, en calidad de agentes, asistidos por los Sres. D. Beard, G. Facenna y J. Eadie, QC, y la Sra. S. Ford, barrister;

— en nombre del Gobierno belga, por los Sres. J.-C. Halleux y S. Vanrie y por la Sra. C. Pochet, en calidad de agentes;

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

— en nombre del Gobierno danés, por el Sr. C. Thorning y la Sra. M. Wolff, en calidad de agentes;

— en nombre del Gobierno alemán, por los Sres. T. Henze y M. Hellmann y por la Sra. J. Kemper, en calidad de agentes, asistidos por los Sres. M. Kottmann y U. Karpenstein, Rechtsanwälte;

— en nombre del Gobierno estonio, por la Sra. K. Kraavi-Käerdi, en calidad de agente;

— en nombre de Irlanda, por las Sras. E. Creedon y L. Williams y por el Sr. A. Joyce, en calidad de agentes, asistidos por el Sr. D. Fennelly, BL;

— en nombre del Gobierno español, por el Sr. A. Rubio González, en calidad de agente;

— en nombre del Gobierno francés, por los Sres. G. de Bergues, D. Colas y F.-X. Bréchot y la Sra. C. David, en calidad de agentes;

— en nombre del Gobierno chipriota, por la Sra. K. Kleanthous, en calidad de agente;

— en nombre del Gobierno húngaro, por los Sres. M. Fehér y G. Koós, en calidad de agentes;

— en nombre del Gobierno neerlandés, por las Sras. M. Bulterman y M. Gijzen y por el Sr. J. Langer, en calidad de agentes;

— en nombre del Gobierno polaco, por el Sr. B. Majczyna, en calidad de agente;

— en nombre del Gobierno finlandés, por el Sr. J. Heliskoski, en calidad de agente;

— en nombre de la Comisión Europea, por los Sres. H. Krämer, K. Simonsson, H. Kranenborg y D. Nardi y las Sras. P. Costa de Oliveira y J. Vondelng, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 19 de julio de 2016;

dicta la siguiente

Sentencia

1 Las peticiones de decisión prejudicial tienen por objeto la interpretación del artículo 15, apartado 1, de la 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) (DO 2002, L 201, p. 37), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (DO 2009, L 337, p. 11) (en lo sucesivo, «Directiva 2002/58»), en relación con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

2 Estas peticiones han sido presentadas en el marco de dos litigios: el primero, entre Tele2 Sverige AB y la Post- och telestyrelsen (autoridad sueca de control de los servicios de correos y telecomunicaciones; en lo sucesivo, «PTS»), en relación con el requerimiento dirigido por esta última a Tele2 Sverige para que procediera a la conservación de los datos de tráfico y de localización de sus abonados y usuarios registrados (asunto C-203/15), y el segundo, entre los Sres. Tom Watson, Peter Brice y Geoffrey Lewis, por un lado, y el Secretary of State for the Home Department (Ministro del Interior, Reino Unido de Gran Bretaña e Irlanda del Norte), por otro, en relación con la conformidad con el Derecho de la Unión del artículo 1 de la Data Retention and Investigatory Powers Act 2014 (Ley de 2014 sobre conservación de datos y facultades de investigación; en lo sucesivo, «DRIPA») (asunto C-698/15).

Marco jurídico

Derecho de la Unión

Directiva 2002/58

3 Los considerandos 2, 6, 7, 11, 21, 22, 26 y 30 de la Directiva 2002/58 establecen:

«(2) La presente Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la [Carta]. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de [ésta].

[...]

(6) Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad.

(7) En el caso de las redes públicas de comunicación, deben elaborarse disposiciones legales, reglamentarias y técnicas específicas con objeto de proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular frente a la creciente capacidad de almacenamiento y tratamiento informático de datos relativos a abonados y usuarios.

[...]

(11) Al igual que 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)], la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según la interpretación que se hace de éste en las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

[...]

(21) Deben adoptarse medidas para evitar el acceso no autorizado a las comunicaciones a fin de proteger la confidencialidad de las mismas, incluidos tanto sus contenidos como cualquier dato relacionado con ellas, por medio de las redes públicas de comunicaciones y los servicios de comunicaciones electrónicas disponibles al público. La legislación nacional de algunos Estados miembros prohíbe solamente el acceso intencionado no autorizado a las comunicaciones.

(22) Al prohibirse el almacenamiento de comunicaciones, o de los datos de tráfico relativos a éstas, por terceros distintos de los usuarios o sin su consentimiento no se pretende prohibir el almacenamiento automático, intermedio y transitorio de esta información, en la medida en que sólo tiene lugar para llevar a cabo la transmisión en la red de comunicaciones electrónicas, y siempre que la información no se almacene durante un período mayor que el necesario para la transmisión y para los fines de la gestión del tráfico, y que durante el período de almacenamiento se garantice la confidencialidad. [...]

[...]

(26) Los datos relativos a los abonados que son tratados en las redes de comunicaciones electrónicas para el establecimiento de conexiones y la transmisión de información contienen información sobre la vida privada de las personas físicas, y afectan al derecho de éstas al respeto de su correspondencia, o se refieren a los intereses legítimos de las personas jurídicas. Dichos datos sólo deben poder almacenarse en la medida en que resulten necesarios para la prestación del servicio, para fines de facturación y para los pagos de interconexión, y durante un tiempo limitado. Cualquier otro tratamiento de dichos datos [...] sólo puede permitirse si el abonado ha manifestado su consentimiento fundado en una información plena y exacta facilitada por el proveedor de servicios de comunicaciones electrónicas disponibles al público acerca del tipo de tratamiento que pretende llevar a cabo y sobre el derecho del abonado a denegar o a retirar su consentimiento a dicho tratamiento. [...]

[...]

(30) Los sistemas para el suministro de redes y servicios de comunicaciones electrónicas deben diseñarse de modo que se limite la cantidad de datos personales al mínimo estrictamente necesario. [...]»

4 El artículo 1 de la Directiva 2002/58, titulado «Ámbito de aplicación y objetivo», dispone:

«1. La presente Directiva establece la armonización de las disposiciones nacionales necesaria para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad.

2. Las disposiciones de la presente Directiva especifican y completan la Directiva [95/46] a los efectos mencionados en el apartado 1. Además, protegen los intereses legítimos de los abonados que sean personas jurídicas.

3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, como las reguladas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal.»

5 Según el artículo 2 de la Directiva 2002/58, con el epígrafe «Definiciones»:

«Salvo disposición en contrario, serán de aplicación a efectos de la presente Directiva las definiciones que figuran en la Directiva [95/46] y en la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) [(DO 2002, L 108, p. 33)].

Además, a efectos de la presente Directiva se entenderá por:

[...]

b) "datos de tráfico": cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;

c) "datos de localización": cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;

d) "comunicación": cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información;

[...]»

6 El artículo 3 de la Directiva 2002/58, titulado «Servicios afectados», establece:

«La presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos.»

7 El artículo 4 de esta Directiva, con el epígrafe «Seguridad del tratamiento», tiene el siguiente tenor:

«1. El proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de comunicaciones por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente.

1 *bis* Sin perjuicio de lo dispuesto en la Directiva [95/46], las medidas a que se refiere el apartado 1, como mínimo:

— garantizarán que solo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley,

— protegerán los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos, y

— garantizarán la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

[...]»

8 Conforme al artículo 5 de la Directiva 2002/58, titulado «Confidencialidad de las comunicaciones»:

«1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad.

[...]

3. Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva [95/46]. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario.»

9 El artículo 6 de la Directiva 2002/58, con el epígrafe «Datos de tráfico», dispone:

«1. Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.

2. Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

El proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido en la medida y durante el tiempo necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento previo. Los usuarios o abonados dispondrán de la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento.

[...]

5. Sólo podrán encargarse del tratamiento de datos de tráfico, de conformidad con los apartados 1, 2, 3 y 4, las personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas o de la prestación de un servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades.»

10 El artículo 9 de esta Directiva, titulado «Datos de localización distintos de los datos de tráfico», establece en su apartado 1:

«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, sólo 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. El proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido. [...]»

11 El artículo 15 de la mencionada Directiva, con el epígrafe «Aplicación de determinadas disposiciones de la Directiva [95/46]», enuncia:

«1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente 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 apartado 1 del artículo 13 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 presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea.

[...]

1 *ter*. Los proveedores instaurarán procedimientos internos para responder a las solicitudes de acceso a los datos personales de los usuarios con arreglo a las disposiciones nacionales promulgadas de conformidad con el apartado 1. Previa solicitud, facilitarán a las autoridades nacionales competentes información sobre esos procedimientos, el número de solicitudes recibidas, la motivación jurídica aducida y la respuesta ofrecida.

2. Las disposiciones del capítulo III sobre recursos judiciales, responsabilidad y sanciones de la Directiva [95/46] se aplicarán a las disposiciones nacionales adoptadas con arreglo a la presente Directiva y a los derechos individuales derivados de la misma.

[...]»

Directiva 95/46

12 El artículo 22 de la Directiva 95/46, que figura en el capítulo III de ésta, tiene el siguiente tenor:

«Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.»

Directiva 2006/24/CE

13 El artículo 1 de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO 2006, L 105, p. 54), con el epígrafe «Objeto y ámbito», establece en su apartado 2:

«La presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.»

14 Con arreglo al artículo 3 de esta Directiva, titulado «Obligación de conservar datos»:

Como excepción a los artículos 5, 6 y 9 de la Directiva [2002/58], los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.

2. La obligación de conservar datos mencionada en el apartado 1 incluirá la conservación de los datos especificados en el artículo 5 en relación con las llamadas telefónicas infructuosas en las que los datos los generan o tratan, y conservan (en lo que a los datos telefónicos se refiere) o registran (en lo que a los datos de Internet se refiere), proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo la jurisdicción del Estado miembro de que se trate en el marco de la prestación de los servicios de comunicaciones en cuestión. La conservación de datos en relación con las llamadas no conectadas no será obligatoria con arreglo a la presente Directiva»

Derecho sueco

15 De la resolución de remisión en el asunto C-203/15 se desprende que el legislador sueco, a efectos de la transposición de la Directiva 2006/24 en el Derecho nacional, modificó la lagen (2003:389) om elektronisk kommunikation [Ley (2003:389) sobre comunicaciones electrónicas; en lo sucesvio, «LEK»] y el förordningen (2003:396) om elektronisk kommunikation [Reglamento (2003:396) sobre comunicaciones electrónicas]. Ambas normas, en su versión aplicable al asunto principal, establecen disposiciones sobre la conservación de los datos relativos a las comunicaciones electrónicas y sobre el acceso a esos datos por las autoridades nacionales.

16 El acceso a dichos datos está regulado, además, por la lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet [Ley (2012:278) sobre la obtención de datos relativos a las comunicaciones electrónicas en el contexto de la actividad de inteligencia de las autoridades encargadas de la lucha contra la delincuencia; en lo sucesivo, «Ley (2012:278)»], y en el rättegångsbalken (Código de procedimiento judicial; en lo sucesivo, «RB»).

Sobre la obligación de conservación de los datos relativos a las comunicaciones electrónicas

17 Según las indicaciones facilitadas por el órgano jurisdiccional remitente en el asunto C-203/15, las disposiciones del artículo 16a del capítulo 6 de la LEK, en relación con el artículo 1 del capítulo 2 de dicha Ley, establecen que los proveedores de servicios de comunicaciones electrónicas deberán

conservar los datos cuya conservación estaba prevista por la Directiva 2006/24. Se trata de los datos relativos a los abonos y a todas las comunicaciones electrónicas necesarios para rastrear e identificar el origen y el destino de una comunicación, para determinar la fecha, la hora, la duración y la naturaleza de dicha comunicación, para identificar el equipo de comunicación utilizado y para localizar el equipo de comunicación móvil utilizado al comienzo y al final de la comunicación. La obligación de conservación de datos se refiere a los datos generados o tratados en relación con servicios telefónicos, servicios telefónicos a través de un punto de conexión móvil, sistemas de mensajería electrónica, servicios de acceso a Internet y servicios de prestación de capacidad de acceso a Internet (modo de conexión). Esta obligación incluye igualmente los datos relativos a las comunicaciones infructuosas. No se refiere, en cambio, al contenido de las comunicaciones.

18 Los artículos 38 a 43 del Reglamento (2003:396) sobre comunicaciones electrónicas concretan las categorías de datos que deben conservarse. Por lo que se refiere a los servicios telefónicos, deberán conservarse, en particular, los datos relativos a las llamadas y a los números llamados, así como las fechas y las horas rastreables en las que comienza y finaliza la comunicación. Respecto a los servicios telefónicos a través de un punto de conexión móvil, se imponen obligaciones complementarias como, por ejemplo, la conservación de los datos de localización del inicio y el final de la comunicación. En relación con los servicios telefónicos que utilizan un paquete IP, además de los datos antes mencionados, deberán conservarse, en particular, los datos relativos a la dirección IP desde la que se llama y a la que se llama. Por lo que se refiere a los sistemas de mensajería electrónica, deberán conservarse, en particular, los datos relativos a los números, las direcciones IP o cualquier otra dirección de mensajería del remitente y del destinatario. Respecto a los servicios de acceso a Internet, deberán conservarse, por ejemplo, los datos relativos a las direcciones IP de los usuarios y las fechas y horas rastreables de la conexión y desconexión al servicio de acceso a Internet.

Sobre la duración de la conservación de los datos

19 Conforme al artículo 16d del capítulo 6 de la LEK, los proveedores de servicios de comunicaciones electrónicas deberán conservar los datos a que se refiere el artículo 16a de dicho capítulo durante seis meses desde el día en que finalice la comunicación. A continuación, deberán ser eliminados inmediatamente, salvo que el artículo 16d, párrafo segundo, disponga otra cosa.

Sobre el acceso a los datos conservados

20 El acceso a los datos conservados por las autoridades nacionales se regula en la Ley (2012:278), la LEK y el RB.

– Ley (2012:278)

21 En el marco de las actividades de inteligencia, la policía nacional, la Säkerhetspolisen (policía de seguridad, Suecia) y la Tullverket (Administración de aduanas, Suecia) podrán, con arreglo al artículo 1 de la Ley (2012:278), de conformidad con los requisitos establecidos en dicha Ley y sin conocimiento del proveedor de una red electrónica de comunicaciones o de un servicio de comunicaciones electrónicas autorizado con arreglo a la LEK, recabar datos relativos a los mensajes transmitidos en una red de comunicaciones electrónicas, a los equipos de comunicación electrónica que se encuentren en una zona geográfica determinada y a la zona o zonas geográficas en las que se sitúe o se haya situado un equipo de comunicación electrónica.

22 Conforme a los artículos 2 y 3 de la Ley (2012:278), podrán obtenerse datos, en principio, cuando, habida cuenta de las circunstancias, la medida sea especialmente necesaria para prevenir, impedir o descubrir actividades delictivas referidas a delitos sancionados con una pena privativa de libertad de dos años por lo menos o a delitos incluidos en la enumeración del artículo 3 de dicha Ley, que

comprende delitos sancionados con una pena privativa de libertad inferior a dos años. Los motivos que justifican dicha medida deben ser superiores a las consideraciones relativas a la injerencia o al perjuicio que se pueda causar a su destinatario o a otros intereses contrapuestos. Con arreglo al artículo 5 de dicha Ley, la medida no podrá durar más de un mes.

23 La decisión de adoptar tal medida corresponde al director de la autoridad de que se trate o a la persona en la que éste haya delegado a estos efectos. Esta decisión no está sujeta al control previo de una autoridad judicial o de una autoridad administrativa independiente.

24 Conforme al artículo 6 de la Ley (2012:278), la Säkerhets och integritetsskyddsnämnden (Comisión de seguridad y protección de la privacidad, Suecia) deberá ser informada de toda decisión por la que se autorice la obtención de datos. El artículo 1 de la lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet [Ley (2007:980) de control de ciertas actividades de lucha contra la delincuencia] establece que dicha autoridad controla la aplicación de la Ley por las autoridades encargadas de la lucha contra la delincuencia.

– LEK

25 El artículo 22, párrafo primero, punto 2, del capítulo 6 de la LEK dispone que los proveedores de servicios de comunicaciones electrónicas deberán comunicar los datos relativos a un abono a petición del Ministerio Fiscal, de la policía nacional, de la policía de seguridad o de cualquier otra autoridad pública encargada de la lucha contra la delincuencia, cuando dichos datos tengan relación con la sospecha de comisión de un delito. Según la información facilitada por el órgano jurisdiccional remitente en el asunto C-203/15, no es necesario que se trate de un delito grave.

– RB

26 El RB regula la comunicación de datos conservados a las autoridades nacionales en el marco de investigaciones preliminares. Conforme al artículo 19 del capítulo 27 del RB, la «vigilancia de las comunicaciones electrónicas» sin conocimiento de terceros está autorizada, en principio, en el marco de las investigaciones preliminares que tengan por objeto, en particular, los delitos sancionados con una pena de privación de libertad de por lo menos seis meses. Por «vigilancia de las comunicaciones electrónicas» se entiende, con arreglo al artículo 19 del capítulo 27 del RB, la obtención de datos sin conocimiento de terceros en relación con los mensajes transmitidos a través de una red de comunicaciones electrónicas, los equipos de comunicación electrónica que se encuentren o hayan estado en una zona geográfica determinada y la zona o zonas geográficas en las que se encuentre o haya habido un equipo de comunicación electrónica concreto.

27 Según los datos facilitados por el órgano jurisdiccional remitente en el asunto C-203/15, con arreglo al artículo 19 del capítulo 27 del RB no puede obtenerse información sobre el contenido de los mensajes. En principio, conforme al artículo 20 del capítulo 27 del RB, sólo es posible ordenar la vigilancia de las comunicaciones electrónicas cuando existan sospechas fundadas de que una persona es el autor de un delito y cuando la medida sea especialmente necesaria para la investigación. Además, dicha investigación debe tener por objeto un delito sancionado con una pena de privación de libertad de dos años por lo menos, así como la tentativa, preparación o conspiración para la comisión de tal delito. Con arreglo al artículo 21 del capítulo 27 del RB, el Ministerio Fiscal deberá solicitar al juez competente, salvo en caso de urgencia, autorización para llevar a cabo la vigilancia de las comunicaciones electrónicas.

Sobre la seguridad y la protección de los datos conservados

28 Conforme al artículo 3a del capítulo 6 de la LEK, los proveedores de servicios de comunicaciones electrónicas que están obligados a conservar datos deben adoptar las medidas técnicas y de gestión adecuadas para garantizar la protección de los datos durante su tratamiento. Sin embargo, según la información facilitada por el tribunal remitente en el asunto C-203/15, el Derecho sueco no establece disposiciones relativas al lugar de conservación de los datos.

Derecho del Reino Unido

DRIPA

29 El artículo 1 de la DRIPA, con el epígrafe «Facultades de conservación de datos de comunicaciones relevantes sujeta a garantías», dispone:

«(1) El [Ministro del Interior] podrá exigir mediante notificación ("notificación de conservación") a un operador de telecomunicaciones públicas que conserve datos de comunicaciones relevantes si considera que ello resulta necesario y proporcionado con respecto a uno o varios de los objetivos comprendidos en las letras a) a h) del artículo 22, apartado 2, de la Ley sobre regulación de las facultades de investigación de 2000 [Regulation of Investigatory Powers Act 2000] (objetivos para los que pueden obtenerse los datos de comunicaciones).

(2) Las notificaciones de conservación podrán:

(a) referirse a un operador concreto o a cualquier tipo de operadores;

(b) exigir la conservación de todos los datos o de cualquier tipo de datos;

(c) especificar el período o períodos durante los cuales deberán conservarse los datos;

(d) contener otros requisitos o restricciones en relación con la conservación de datos;

(e) establecer disposiciones diferentes para fines diferentes;

(f) referirse a datos que existan o no en el momento de la expedición o de la entrada en vigor de la notificación.

(3) El [Ministro del Interior] podrá establecer mediante reglamento disposiciones adicionales sobre la conservación de datos de comunicaciones relevantes.

(4) Esas disposiciones podrán establecer, en particular:

(a) requisitos previos a la expedición de una notificación de conservación;

(b) el período máximo durante el cual los datos deben ser conservados en virtud de una notificación de conservación;

(c) el contenido, la expedición, la entrada en vigor, la revisión, la modificación o la revocación de una notificación de conservación;

(d) la integridad, la seguridad o la protección, el acceso, la comunicación o la destrucción de datos conservados en virtud del presente artículo;

(e) la aplicación o el control del cumplimiento de los requisitos o restricciones pertinentes;

(f) un código de buenas prácticas en relación con los requisitos, restricciones o facultades relevantes;

(g) el reembolso por el [Ministro del Interior] (con sujeción o no a condiciones) de los gastos soportados por los operadores de telecomunicaciones públicas por el cumplimiento de los requisitos o restricciones pertinentes;

(h) el fin de la vigencia del [Data Retention (EC Directive) Regulations 2009 (Reglamento de 2009 sobre la conservación de datos en el sentido de la Directiva CE)] y la transición hacia la conservación de datos en virtud del presente artículo.

(5) El período máximo establecido en virtud del apartado 4, letra b), no deberá superar 12 meses contados a partir de la fecha determinada en relación con los datos de que se trate por el reglamento mencionado en el apartado 3.

[...] »

30 El artículo 2 de la DRIPA define la expresión «datos de comunicaciones relevantes» como «datos de comunicaciones del tipo de las mencionadas en el anexo del Reglamento de 2009 sobre la conservación de datos en el sentido de la Directiva CE, en la medida en que tales datos sean generados o tratados en el Reino Unido por operadores de telecomunicaciones públicas en el marco de la prestación de los servicios de telecomunicaciones en cuestión».

RIPA

31 El artículo 21 de la Ley de 2000 sobre la regulación de las facultades de investigación (en lo sucesivo, «RIPA»), que figura en el capítulo II de dicha Ley y lleva el epígrafe «Obtención y divulgación de datos de comunicaciones», precisa en su apartado 4:

«A efectos del presente capítulo, "datos de comunicaciones" tendrá cualquiera de los significados siguientes:

(a) cualesquiera datos sobre tráfico contenidos o adjuntos a una comunicación (ya sea por el remitente o de cualquier otro modo) a efectos de cualquier servicio postal o sistema de telecomunicación por medio del cual sean o puedan ser transmitidos;

(b) cualquier información que no incluye ningún contenido de una comunicación [aparte de la información mencionada en la letra (a)] y que haga referencia al uso que cualquier persona realice:
  (i) de cualquier servicio postal o de telecomunicaciones, o
  (ii) en relación con la prestación a cualquier persona, o el uso por ella, de un servicio de telecomunicaciones o de cualquier parte de un sistema de telecomunicaciones;

(c) cualquier información no comprendida en las letras a) o b) que una entidad que preste un servicio postal o de telecomunicaciones posea u obtenga sobre personas a las que preste servicio».

32 Según las indicaciones contenidas en la resolución de remisión en el asunto C-698/15, esos datos incluyen los «datos de localización de un usuario», pero no los datos relativos al contenido de una comunicación.

33 En cuanto al acceso a los datos conservados, el artículo 22 de la RIPA establece:

«(1) Este artículo será aplicable cuando la persona responsable a efectos de este capítulo estime que es necesario obtener datos de comunicaciones por los motivos enumerados en el apartado 2.

(2) Será necesario obtener datos de comunicaciones por los motivos enumerados en el presente apartado si estos son necesarios:

(a) en interés de la seguridad nacional;

(b) para impedir o detectar la comisión de delitos o impedir desórdenes públicos;

(c) en interés del bienestar económico del Reino Unido;

(d) en interés de la seguridad pública;

(e) para la protección de la salud pública;

(f) para liquidar o recaudar cualquier impuesto, tasa, carga u otro tributo, contribución o gravamen debido a la Administración pública;

(g) para impedir, en caso de emergencia, el fallecimiento, lesiones o cualquier daño a la salud física o mental de una persona, así como para atenuar cualquier lesión o daño a la salud física o mental de una persona;

(h) con cualquier otro fin [no comprendido en las letras (a) a (g)] establecido en una orden dictada por el [Ministro del Interior].

(4) Sin perjuicio del apartado 5, cuando la persona responsable considere que un operador de telecomunicaciones o un operador postal posee datos o podría poseerlos, o podría obtenerlos, podrá exigirle, mediante requerimiento, que

(a) obtenga los datos, si aún no obran en su poder, y

(b) divulgue, en todo caso, todos los datos que posea o que haya obtenido posteriormente.

(5) La persona responsable sólo dará su autorización conforme al apartado 3 o dictará un requerimiento conforme al apartado 4 si considera que la obtención de los datos en cuestión resultante de un comportamiento autorizado o exigido en virtud de una autorización o requerimiento es proporcionada a la finalidad perseguida por la obtención de datos.»

34 Con arreglo al artículo 65 de la RIPA, podrán presentarse reclamaciones ante el Investigatory Powers Tribunal (Tribunal encargado de las facultades de investigación, Reino Unido) si existen motivos para pensar que los datos han sido obtenidos de modo inapropiado.

El Data Retention Regulations 2014

35 El Data Retention Regulations 2014 (Reglamento de 2014 sobre la conservación de datos), adoptado sobre la base de la DRIPA, está dividido en tres partes. La segunda comprende los artículos 2 a 14 de ese Reglamento. El artículo 4, con el epígrafe «Requerimientos en materia de conservación», establece:

«(1) Los requerimientos en materia de conservación deberán precisar:

(a) el operador público de telecomunicaciones (o la descripción de los operadores) al que se dirigen,

(b) los datos de comunicaciones relevantes que deben ser conservados,

(c) el período o los períodos durante los cuales deben conservarse los datos,

(d) cualquier otro requisito o restricción en relación con la conservación de datos.

(2) Un requerimiento en materia de conservación de datos no podrá exigir que un dato se conserve más de 12 meses desde:

(a) en los casos de datos de tráfico o de datos relativos a la utilización del servicio, el día de la comunicación de que se trate, y

(b) en el caso de datos relativos a los abonados, el día en el que la persona afectada ponga fin al servicio de comunicación de que se trate o el día en el que se modifique el dato (si este último es anterior).

[...]»

36 Según el artículo 7 de ese Reglamento, que lleva el epígrafe «Integridad y seguridad de los datos»:

«(1) El operador público de telecomunicaciones que conserve datos con arreglo al artículo 1 de la [DRIPA] deberá:

(a) garantizar que los datos tengan la misma integridad y estén sujetos por lo menos al mismo nivel de seguridad y de protección que los datos de los sistemas de los que proceden,

(b) garantizar, mediante medidas técnicas y de gestión apropiadas, que sólo el personal especialmente autorizado podrá tener acceso a los datos, y

(c) proteger, mediante medidas técnicas y de gestión apropiadas, los datos frente a la destrucción ilícita, las pérdidas o los daños de origen accidental, o frente a la conservación, el tratamiento, el acceso o la divulgación ilícitos o no autorizados.

(2) El operador público de telecomunicaciones que conserve datos de comunicaciones con arreglo al artículo 1 de la [DRIPA] deberá destruir los datos si su conservación deja de estar autorizada por este artículo y no está autorizada de algún otro modo por la Ley.

(3) La exigencia prevista en el apartado 2 de destruir los datos es una exigencia que consiste en eliminar los datos de modo que sea imposible acceder a ellos.

(4) Basta con que el operador adopte medidas para la eliminación de los datos con carácter mensual o en períodos más cortos según las posibilidades del operador en la práctica.»

37 El artículo 8 de dicho Reglamento, con el epígrafe «Divulgación de datos conservados», establece:

«(1) El operador público de telecomunicaciones debe establecer sistemas de seguridad adecuados (que incluyan medidas técnicas y de gestión) que determinen el acceso a los datos de comunicaciones conservados con arreglo al artículo 1 de la [DRIPA] para evitar cualquier divulgación no comprendida en el artículo 1, apartado 6, letra a), de la [DRIPA]

(2) El operador público de telecomunicaciones que conserve datos con arreglo al artículo 1 de la [DRIPA] deberá conservar los datos de modo que pueda transmitirlos, sin retraso injustificado, en respuesta a requerimientos.»

38 El artículo 9 de ese mismo Reglamento, que lleva el epígrafe «Control del comisario encargado de la información», dispone:

«El comisario encargado de la información deberá controlar el cumplimiento de los requisitos o restricciones, previstos en esta parte, en relación con la integridad, la seguridad y la destrucción de datos conservados con arreglo al artículo 1 de la [DRIPA]»

Código de buenas prácticas

39 El Acquisition and Disclosure of Communications Data Code of Practice (Código de buenas prácticas sobre obtención y divulgación de datos de comunicaciones; en lo sucesivo, «Código de buenas prácticas») contiene, en sus apartados 2.5 a 2.9 y 2.36 a 2.45, orientaciones sobre la necesidad y la proporcionalidad de la obtención de datos de comunicaciones. Según las explicaciones proporcionadas por el tribunal remitente en el asunto C-698/15, debe prestarse una especial atención, conforme a los apartados 3.72 a 3.77 de dicho Código, a la necesidad y a la proporcionalidad cuando los datos de comunicaciones solicitados se refieran a una persona que sea miembro de una profesión que dispone de información protegida por el secreto profesional o que es confidencial por algún otro motivo.

40 En virtud de los apartados 3.78 a 3.84 de dicho Código, se requiere una orden judicial en el caso especial de solicitud de datos de comunicaciones realizada para identificar las fuentes de los periodistas. Según los apartados 3.85 a 3.87 de ese mismo Código, en caso de solicitud de acceso formulada por autoridades locales es necesaria una aprobación judicial. En cambio, no se precisa ninguna autorización emitida por un juez o por una entidad independiente para acceder a datos de comunicaciones protegidos por el secreto profesional de los abogados, médicos, miembros del Parlamento o ministros de cultos religiosos.

41 El apartado 7.1 del Código de buenas prácticas prevé que los datos de comunicaciones logrados u obtenidos en virtud de las disposiciones de la RIPA así como todos los extractos, resúmenes y copias de esos datos deberán ser tratados y almacenados de manera segura. Además, deben cumplirse los requisitos que figuran en la Data Protection Act (Ley relativa a la protección de datos).

42 Conforme al apartado 7.18 del Código de buenas prácticas, cuando una autoridad pública del Reino Unido se plantea la posibilidad de divulgar a autoridades extranjeras datos de comunicaciones, deberá, en particular, examinar si dichos datos van a ser protegidos de modo adecuado. No obstante, del apartado 7.22 de dicho Código se desprende que podrá realizarse una transmisión de datos a un país tercero cuando dicha transmisión sea necesaria por motivos de interés público sustancial aun cuando ese país tercero no garantice un nivel de protección adecuado. Según indica el tribunal remitente en el asunto C-698/15, el Ministro del Interior podrá expedir un certificado de seguridad nacional por el que se exima a ciertos datos del cumplimiento de las disposiciones previstas en la legislación.

43 En el apartado 8.1 del citado Código se recuerda que la RIPA instituyó la Interception of Communications Commissioner (Comisario para la interceptación de las comunicaciones, Reino Unido), cuya función consiste, en particular, en supervisar de modo independiente el ejercicio y la aplicación de las facultades y deberes enunciados en el capítulo II de la parte I de la RIPA. Como se desprende del apartado 8.3 de ese mismo Código, cuando el mencionado comisario pueda «acreditar que una persona ha sido perjudicada por un incumplimiento voluntario o por imprudencia» podrá informar a esta persona de que existe la sospecha de un uso ilícito de facultades.

Litigios principales y cuestiones prejudiciales

Asunto C-203/15

44 El 9 de abril de 2014, Tele2 Sverige, proveedor de servicios de comunicaciones electrónicas establecido en Suecia, notificó a la PTS que, a raíz de la invalidación de la Directiva 2006/24 mediante la sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12; en lo sucesivo, «sentencia Digital Rights», EU:C:2014:238), no seguiría conservando, a partir del 14 de abril de 2014, los datos de comunicaciones electrónicas a que se refiere la LEK, y que suprimiría los datos conservados hasta esa fecha.

45 El 15 de abril de 2014, la Rikspolisstyrelsen (Dirección General de la Policía Nacional, Suecia) presentó una queja ante la PTS porque Tele2 Sverige había dejado de comunicarle los datos de que se trata.

46 El 29 de abril de 2014, el justitieminister (Ministro de Justicia, Suecia) designó a un asesor especial para que analizara la normativa sueca controvertida a la luz de la sentencia Digital Rights. En un informe de 13 de junio de 2014, titulado «Datalagring, EU-rätten och svensk rätt, n.º Ds 2014:23» (Conservación de datos, Derecho de la Unión y Derecho sueco; en lo sucesivo, «Informe de 2014»), el asesor especial llegó a la conclusión de que la normativa nacional relativa a la conservación de datos, tal como estaba establecida en los artículos 16a a 16f de la LEK, no era contraria al Derecho de la Unión ni al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950 (en lo sucesivo, «CEDH»). El asesor especial señaló que la sentencia Digital Rights no podía interpretarse en el sentido de que hubiera censurado el propio principio de la conservación generalizada e indiferenciada de datos. Desde su punto de vista, la sentencia Digital Rights tampoco podía entenderse en el sentido de que el Tribunal de Justicia hubiera sentado en ella una serie de criterios que debieran cumplirse en su totalidad para que una normativa pudiera considerarse proporcionada. En su opinión, deben apreciarse todas las circunstancias para determinar la conformidad de la normativa sueca con el Derecho de la Unión, como el alcance de la conservación de los datos a la vista de las disposiciones sobre el acceso a los datos, la duración de su conservación, su protección y su seguridad.

47 Sobre esta base, el 19 de junio de 2014, la PTS comunicó a Tele2 Sverige que estaba incumpliendo las obligaciones previstas en la normativa nacional al no conservar los datos a que se refiere la LEK durante seis meses a efectos de la lucha contra la delincuencia. A continuación, mediante requerimiento de 27 de junio de 2014, la PTS le ordenó que volviera a conservar esos datos a más tardar a partir del 25 de julio de 2014.

48 Al estimar que el Informe de 2014 se basaba en una interpretación incorrecta de la sentencia Digital Rights y que la obligación de conservación de datos era contraria a los derechos fundamentales garantizados en la Carta, Tele2 Sverige interpuso un recurso ante el Förvaltningsrätten i Stockholm (Tribunal de lo Contencioso-Administrativo de Estocolmo, Suecia) contra el requerimiento de 27 de junio de 2014. Dicho tribunal desestimó el recurso mediante sentencia de 13 de octubre de 2014. A continuación, Tele2 Sverige apeló dicha sentencia ante el órgano jurisdiccional remitente.

49 Según el órgano jurisdiccional remitente, la compatibilidad de la normativa sueca con el Derecho de la Unión debe apreciarse a la luz del artículo 15, apartado 1, de la Directiva 2002/58. En su opinión, aunque esta Directiva establece el principio de que los datos de tráfico y de localización deben eliminarse o hacerse anónimos cuando ya no son necesarios para la transmisión de una comunicación, el artículo 15, apartado 1, de dicha Directiva introduce una excepción a dicho principio al autorizar a los Estados miembros, cuando esté justificado por alguno de los motivos que enuncia, a limitar esa obligación de eliminación o de anonimización o también a prever la conservación de los datos. Afirma que el Derecho de la Unión permite que se conserven datos de comunicaciones electrónicas en determinadas situaciones.

50 El órgano jurisdiccional remitente se pregunta, no obstante, si una obligación generalizada e indiferenciada de conservación de datos de comunicaciones electrónicas, como la controvertida en el asunto principal, es compatible, habida cuenta de la sentencia Digital Rights, con el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 52, apartado 1, de la Carta. Puesto que las partes tienen opiniones divergentes sobre esta cuestión, el tribunal remitente estima necesario que el Tribunal de Justicia se pronuncie claramente sobre si, como considera Tele2 Sverige, la conservación generalizada e indiferenciada de datos de comunicaciones electrónicas es en sí misma incompatible con los artículos 7, 8 y 52, apartado 1, de la Carta, o si, como se desprende del Informe de 2014, la compatibilidad de tal conservación de datos debe apreciarse con arreglo a las disposiciones relativas al acceso a los datos, a su protección, a su seguridad y a la duración de su conservación.

51 En estas circunstancias, el tribunal remitente ha decidido suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) Una obligación general de conservar datos de tráfico que se refiere a todas las personas, todos los medios de comunicación electrónica y todos los datos de tráfico sin establecer ninguna distinción, limitación o excepción en función del objetivo de la lucha contra la delincuencia [...], ¿es compatible con el artículo 15, apartado 1, de la Directiva 2002/58/CE, habida cuenta de los artículos 7, 8 y 52, apartado 1, de la Carta?

2) En caso de respuesta negativa a la primera cuestión, ¿puede en todo caso ser admisible la conservación:
   a) si el acceso de las autoridades nacionales a los datos conservados se determina como se describe en los apartados 19 a 36 [de la resolución de remisión], y
   b) si las exigencias de protección y de seguridad se regulan como se describe en los apartados 38 a 43 [de la resolución de remisión], y
   si todos los datos de que se trata deben conservarse durante seis meses contados a partir del día en que haya finalizado la comunicación y posteriormente destruirse como se describe en el apartado 37 [de la resolución de remisión]?»

Asunto C-698/15

52 Los Sres. Watson, Brice y Lewis presentaron individualmente ante la High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [Tribunal Superior de Justicia (Inglaterra y País de Gales) (Sección de lo Contencioso-Administrativo) (Reino Unido)], sendos recursos contencioso-administrativos por los que solicitaban el control de la legalidad del artículo 1 de la DRIPA, invocando en particular la incompatibilidad de dicho artículo con los artículos 7 y 8 de la Carta y con el artículo 8 del CEDH.

53 Mediante sentencia de 17 de julio de 2015, la High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [Tribunal Superior de Justicia (Inglaterra y País de Gales) (Sección de lo Contencioso-Administrativo)], declaró que la sentencia Digital Rights enunciaba «requisitos

imperativos de Derecho de la Unión» aplicables a las normativas de los Estados miembros en materia de conservación de datos de comunicaciones así como de acceso a dichos datos. Según dicho órgano jurisdiccional, puesto que el Tribunal de Justicia, en la citada sentencia, había estimado que la Directiva 2006/24 era incompatible con el principio de proporcionalidad, una normativa nacional que tuviera un contenido idéntico al de dicha Directiva tampoco podía ser compatible con ese principio. En su opinión, de la lógica subyacente en la sentencia Digital Rights se desprende que una normativa que establece un régimen generalizado de conservación de datos de comunicaciones vulnera los derechos garantizados en los artículos 7 y 8 de la Carta, salvo que esa normativa se complete con un régimen de acceso a los datos, definido por el Derecho nacional, que prevea suficientes garantías para la salvaguarda de esos derechos. Por tanto, estima que el artículo 1 de la DRIPA no es compatible con los artículos 7 y 8 de la Carta, puesto que no establece normas claras y precisas en relación con el acceso y la utilización de esos datos conservados y no supedita el acceso a dichos datos a un control previo llevado a cabo por un órgano jurisdiccional o por una entidad administrativa independiente.

54 El Ministro del Interior apeló esa sentencia ante la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil) (Reino Unido)].

55 Ese órgano jurisdiccional señala que el artículo 1, apartado 1, de la DRIPA faculta al Ministro del Interior para adoptar, sin autorización previa de un órgano jurisdiccional o de una entidad administrativa independiente, un régimen general que imponga a los operadores de telecomunicaciones públicas la obligación de conservar todos los datos relativos a todo servicio postal o a todo servicio de telecomunicaciones durante un período máximo de doces meses siempre que estime que tal exigencia es necesaria y proporcionada para lograr los fines enunciados en la normativa del Reino Unido. Aunque dichos datos no incluyen el contenido de las comunicaciones, podrían injerir de modo especial en la vida privada de los usuarios de los servicios de comunicaciones.

56 En la resolución de remisión y en su sentencia de 20 de noviembre de 2015, dictada en el procedimiento de apelación y en la que decidió plantear al Tribunal de Justicia la presente petición de decisión prejudicial, el órgano jurisdiccional remitente considera que a las normas nacionales relativas a la conservación de datos se les aplica necesariamente el artículo 15, apartado 1, de la Directiva 2002/58 y que dichas normas deben cumplir los requisitos derivados de la Carta. No obstante, el tribunal remitente estima que, conforme al artículo 1, apartado 3, de dicha Directiva, el legislador de la Unión no armonizó las normas relativas al acceso a los datos conservados.

57 Por lo que se refiere a la incidencia de la sentencia Digital Rights en las cuestiones suscitadas en el litigio principal, el tribunal remitente señala que, en el asunto en el que se dictó dicha sentencia, el Tribunal de Justicia se pronunció sobre la validez de la Directiva 2006/54, y no sobre la validez de una normativa nacional. Habida cuenta, en particular, de la estrecha relación existente entre la conservación de datos y el acceso a dichos datos, era esencial que esta Directiva llevase aparejada una serie de garantías y que la sentencia Digital Rights analizara, al examinar la legalidad del régimen de conservación de datos establecido por la citada Directiva, las normas relativas al acceso a dichos datos. Por tanto, considera que el Tribunal de Justicia no pretendió enunciar en la sentencia requisitos imperativos aplicables a las normativas nacionales sobre el acceso a los datos que no cumplieran el Derecho de la Unión. Además, el razonamiento del Tribunal de Justicia estaba estrechamente ligado al objetivo perseguido por esa misma Directiva. No obstante, en opinión del tribunal remitente, una normativa nacional debe apreciarse a la luz de sus objetivos y de su contexto.

58 En relación con la necesidad de plantear ante el Tribunal de Justicia una petición de decisión prejudicial, el órgano jurisdiccional remitente destaca el hecho de que, en la fecha de adopción de la resolución de remisión, seis tribunales de otros Estados miembros, cinco de ellos de última instancia, habían anulado normativas nacionales basándose en la sentencia Digital Rights. El tribunal remitente considera que la respuesta a las cuestiones prejudiciales planteadas no es evidente y que es necesaria para dirimir los litigios de los que conoce.

59 En estas circunstancias, la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil)] ha decidido suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Establece la sentencia Digital Rights (en particular sus apartados 60 a 62) requisitos imperativos de Derecho de la Unión que resulten aplicables al régimen nacional de un Estado miembro que regula el acceso a los datos conservados de conformidad con la legislación nacional, al objeto de dar cumplimiento a los artículos 7 y 8 de la Carta?

2) ¿Amplía la sentencia Digital Rights el alcance de los artículos 7 u 8 de la Carta más allá del alcance del artículo 8 del CEDH, como se establece en la jurisprudencia del Tribunal Europeo de Derechos Humanos?»

Sobre el procedimiento ante el Tribunal de Justicia

60 Mediante auto de 1 de febrero de 2016, Davis y otros (C-698/15, no publicado, EU:C:2016:70), el Presidente del Tribunal de Justicia acordó estimar la solicitud de la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil)] de tramitar el asunto C-698/15 por el procedimiento acelerado establecido en el artículo 105, apartado 1, del Reglamento de Procedimiento del Tribunal de Justicia.

61 Mediante decisión del Presidente del Tribunal de Justicia de 10 de marzo de 2016, se ordenó la acumulación de los asuntos C-203/15 y C-698/15 a efectos de la fase oral y de la sentencia.

Sobre las cuestiones prejudiciales

Sobre la primera cuestión prejudicial en el asunto C-203/15

62 Mediante su primera cuestión prejudicial en el asunto C-203/15, el Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo) solicita, en esencia, que se dilucide si el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional, como la controvertida en el asunto principal, que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.

63 Esta cuestión prejudicial tiene su origen, en particular, en el hecho de que la Directiva 2006/24, que la normativa nacional controvertida en el asunto principal tiene por objeto transponer, fue declarada inválida mediante la sentencia Digital Rights, pero las partes no están de acuerdo en cuanto al alcance de dicha sentencia y a sus efectos sobre dicha normativa. Esta normativa regula tanto la conservación de los datos de tráfico y de localización como el acceso a dichos datos por las autoridades nacionales.

64 Procede examinar previamente si una normativa nacional como la controvertida en el asunto principal está comprendida en el ámbito de aplicación del Derecho de la Unión.

Sobre el ámbito de aplicación de la Directiva 2002/58

65 Los Estados miembros que han presentado observaciones escritas ante el Tribunal de Justicia han expresado opiniones divergentes en cuanto a la cuestión de si las normativas nacionales relativas a la conservación de los datos de tráfico y de localización y al acceso a dichos datos por las autoridades

nacionales, con la finalidad de luchar contra la delincuencia, están comprendidas en el ámbito de aplicación de la Directiva 2002/58, y en su caso en qué medida. En efecto, mientras que, en particular, los Gobiernos belga, danés, alemán, estonio, de Irlanda y neerlandés han manifestado que debe responderse afirmativamente a esta cuestión, el Gobierno checo propone que se responda de modo negativo, observando que esas normativas sólo tienen como objetivo la lucha contra la delincuencia. Por su parte, el Gobierno del Reino Unido alega que sólo están comprendidas en el ámbito de aplicación de la citada Directiva las normativas relativas a la conservación de datos y no las relativas al acceso a esos datos por las autoridades nacionales competentes en materia de lucha contra la delincuencia.

66 Finalmente, la Comisión, si bien sostuvo, en las observaciones escritas presentadas ante el Tribunal de Justicia en el asunto C-203/15, que la normativa nacional controvertida en el asunto principal está comprendida en el ámbito de aplicación de la Directiva 2002/58, en las observaciones escritas presentadas en el asunto C-698/15 indicó que solamente las normas nacionales relativas a la conservación de datos, y no las relativas al acceso de las autoridades nacionales a dichos datos, están comprendidas en el ámbito de aplicación de dicha Directiva. No obstante, en su opinión, estas últimas normas deben tomarse en consideración para apreciar si una normativa nacional que regula la conservación de datos por los proveedores de servicios de comunicaciones electrónicos constituye una injerencia proporcionada en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta.

67 A este respecto, debe señalarse que el alcance del ámbito de aplicación de la Directiva 2002/58 debe apreciarse teniendo en cuenta en especial la sistemática de esta última.

68 Conforme a su artículo 1, apartado 1, la Directiva 2002/58 prevé, concretamente, la armonización de las disposiciones nacionales necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales, en particular del derecho a la intimidad y a la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas.

69 El artículo 1, apartado 3, de esta Directiva excluye de su ámbito de aplicación las «actividades del Estado» en los sectores que enumera, a saber, en concreto, las actividades del Estado en materia penal y las relativas a la seguridad pública, la defensa y la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) (véanse, por analogía, respecto al artículo 3, apartado 2, primer guion, de la Directiva 95/46, las sentencias de 6 de noviembre de 2003, Lindqvist, C-101/01, EU:C:2003:596, apartado 43, y de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 41).

70 En cuanto al artículo 3 de la Directiva 2002/58, éste enuncia que dicha Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Unión, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos (en lo sucesivo, «servicios de comunicaciones electrónicas»). Por tanto, debe considerarse que la citada Directiva regula las actividades de los proveedores de tales servicios.

71 El artículo 15, apartado 1, de la Directiva 2002/58 autoriza a los Estados miembros a adoptar, cumpliendo los requisitos que establece, «medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de [esta] Directiva». El artículo 15, apartado 1, segunda frase, de dicha Directiva indica, como ejemplo de medidas que pueden ser adoptadas por los Estados miembros, medidas «que prevean la conservación de datos».

72 Ciertamente, las medidas legales contempladas en el artículo 15, apartado 1, de la Directiva 2002/58 se refieren a actividades propias de los Estados o de las autoridades estatales, ajenas a los ámbitos de actividad de los particulares (véase, en ese sentido, la sentencia de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartado 51). Además, las finalidades a las que deben responder tales medidas en virtud de dicha disposición, en el presente caso la salvaguarda de la seguridad nacional, de la defensa y de la seguridad pública, así como la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas, coinciden en esencia con las finalidades que persiguen las actividades mencionadas en el artículo 1, apartado 3, de dicha Directiva.

73 Sin embargo, a la vista de la sistemática de la Directiva 2002/58, los elementos señalados en el apartado anterior de la presente sentencia no permiten llegar a la conclusión de que las medidas legales contempladas en el artículo 15, apartado 1, de la Directiva 2002/58 están excluidas del ámbito de aplicación de dicha Directiva, ya que esto privaría de toda eficacia a dicha disposición. En efecto, esta disposición presupone necesariamente que las medidas nacionales que se mencionan en ella, como las relativas a la conservación de datos a efectos de la lucha contra la delincuencia, están comprendidas en el ámbito de aplicación de esa misma Directiva, dado que ésta sólo autoriza expresamente a los Estados miembros a adoptarlas cumpliendo los requisitos que establece.

74 Por otro lado, las medidas legales a que se refiere el artículo 15, apartado 1, de la Directiva 2002/58 regulan, a los efectos mencionados en dicha disposición, la actividad de los proveedores de servicios de comunicaciones electrónicas. Por tanto, ese artículo 15, apartado 1, en relación con el artículo 3 de dicha Directiva, debe interpretarse en el sentido de que tales medidas legales están comprendidas en el ámbito de aplicación de la misma Directiva.

75 En particular, queda comprendida en ese ámbito de aplicación una medida legal, como la controvertida en el asunto principal, que impone a esos proveedores la obligación de conservar los datos de tráfico y de localización, puesto que dicha actividad implica necesariamente el tratamiento, por ellos, de datos personales.

76 También está incluida en ese ámbito de aplicación una medida legal que regula, como en el asunto principal, el acceso de las autoridades nacionales a los datos conservados por los proveedores de servicios de comunicaciones electrónicas.

77 En efecto, la protección de la confidencialidad de las comunicaciones electrónicas y de sus datos de tráfico, garantizada por el artículo 5, apartado 1, de la Directiva 2002/58, se aplica a las medidas adoptadas por todas las personas distintas de los usuarios, ya sean personas físicas o entidades privadas o públicas. Como confirma el considerando 21 de dicha Directiva, ésta tiene como objetivo evitar «[todo] acceso» no autorizado a las comunicaciones, incluido «todo dato relativo a esas comunicaciones», para proteger la confidencialidad de las comunicaciones electrónicas.

78 En estas circunstancias, una medida legal por la que un Estado miembro impone, con arreglo al artículo 15, apartado 1, de la Directiva 2002/58, a los proveedores de servicios de comunicaciones electrónicas, a los efectos mencionados en esa disposición, la obligación de proporcionar a las autoridades nacionales, conforme a los requisitos previstos por tal medida, el acceso a los datos conservados por dichos proveedores, es una medida que tiene por objeto el tratamiento de datos personales por estos últimos, tratamientos que están comprendidos en el ámbito de aplicación de esta Directiva.

79 Por lo demás, puesto que los datos sólo se conservan con la finalidad de hacerlos accesibles, en su caso, a las autoridades nacionales competentes, una normativa nacional que prevé la conservación de datos implica, en principio, necesariamente la existencia de disposiciones relativas al acceso de las autoridades nacionales competentes a los datos conservados por los proveedores de servicios de comunicaciones electrónicas.

80 Esta interpretación se ve corroborada por el artículo 15, apartado 1 *ter*, de la Directiva 2002/58, según el cual los proveedores instaurarán procedimientos internos para responder a las solicitudes de acceso a los datos personales de los usuarios con arreglo a las disposiciones nacionales promulgadas de conformidad con el apartado 1 del artículo 15 de dicha Directiva.

81 De lo que precede resulta que una normativa nacional como la controvertida en los asuntos principales C-203/15 y C-698/15, está comprendida en el ámbito de aplicación de la Directiva 2002/58.

Sobre la interpretación del artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta

82 Procede señalar que, conforme al artículo 1, apartado 2, de la Directiva 2002/58, las disposiciones de ésta «especifican y completan» la Directiva 95/46. Tal como enuncia su considerando 2, la Directiva 2002/58 tiene como finalidad garantizar, en especial, el pleno respeto de los derechos establecidos en los artículos 7 y 8 de la Carta. A este respecto, de la exposición de motivos de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas [COM(2000) 385 final], origen de la Directiva 2002/58, se desprende que el legislador de la Unión pretendía que «[siguiera] estando garantizado un nivel elevado de protección de los datos personales y la intimidad para todos los servicios de comunicaciones electrónicas con independencia de la tecnología utilizada»

83 Con este fin, la Directiva 2002/58 establece disposiciones específicas que tienen como objetivo, como se desprende en particular de sus considerandos 6 y 7, proteger a los usuarios de servicios de comunicaciones electrónicas frente a los riesgos que suponen para los datos personales y la intimidad las nuevas tecnologías y la creciente capacidad de almacenamiento y tratamiento informático de datos.

84 En particular, el artículo 5, apartado 1, de esta Directiva prevé que los Estados miembros deberán garantizar, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público.

85 El principio de confidencialidad de las comunicaciones establecido por la Directiva 2002/58 implica, entre otros, como se desprende del artículo 5, apartado 1, segunda frase, de ésta, una prohibición, dirigida, en principio, a todas las personas distintas de los usuarios, de almacenar sin el consentimiento de éstos los datos de tráfico relativos a las comunicaciones electrónicas. Sólo se exceptúan las personas legalmente autorizadas de conformidad con el artículo 15, apartado 1, de esta Directiva y el almacenamiento técnico necesario para la conducción de una comunicación (véase, en ese sentido, la sentencia de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartado 47).

86 Así, y como confirman los considerandos 22 y 26 de la Directiva 2002/58, en virtud del artículo 6 de esta Directiva, el tratamiento y el almacenamiento de los datos de tráfico sólo están autorizados en la medida y durante el tiempo necesarios para la facturación de los servicios, la comercialización de éstos y la prestación de servicios con valor añadido (véase, en ese sentido, la sentencia de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartados 47 y 48). Por lo que se refiere, en particular, a la facturación de los servicios, tal tratamiento sólo estará autorizado hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. Una vez expirado este plazo, los datos que hayan sido tratados y almacenados deberán eliminarse o hacerse anónimos. En relación con los datos de localización distintos de los datos de tráfico, el artículo 9, apartado 1, de dicha Directiva establece que esos datos sólo podrán tratarse conforme a ciertos requisitos y tras haberse hecho anónimos o previo consentimiento de los usuarios o abonados.

87 El alcance de las disposiciones de los artículos 5, 6 y 9, apartado 1, de la Directiva 2002/58, que tienen como finalidad garantizar la confidencialidad de las comunicaciones y de los datos relativos a ellas, y minimizar los riesgos de abuso, debe apreciarse además a la luz del considerando 30 de esta Directiva, conforme al cual «los sistemas para el suministro de redes y servicios de comunicaciones electrónicas deben diseñarse de modo que se limite la cantidad de datos personales al mínimo estrictamente necesario».

88 Ciertamente, el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros establecer excepciones a la obligación de principio, enunciada en el artículo 5, apartado 1, de esta Directiva, de garantizar la confidencialidad de los datos personales y a las obligaciones correspondientes, mencionadas concretamente en los artículos 6 y 7 de dicha Directiva (véase, en ese sentido, la sentencia de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartado 50).

89 No obstante, puesto que el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros limitar el alcance de la obligación de principio de garantizar la confidencialidad de las comunicaciones y de los datos de tráfico relativos a ellas, debe interpretarse en sentido estricto conforme a reiterada jurisprudencia del Tribunal de Justicia (véase, por analogía, la sentencia de 22 de noviembre de 2012, Probst, C-119/12, EU:C:2012:748, apartado 23). Por tanto, esta disposición no puede justificar que la excepción a esta obligación de principio y, en particular, a la prohibición de almacenar datos, prevista en el artículo 5 de dicha Directiva, se convierta en la regla si no se quiere privar en gran medida a esta última disposición de su alcance.

90 A este respecto, debe señalarse que el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 prevé que las medidas legales a las que se refiere, y que suponen una excepción al principio de confidencialidad de las comunicaciones y de los datos de tráfico relativos a ellas, deben tener como finalidad «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», o deben perseguir alguno de los demás objetivos contemplados en el artículo 13, apartado 1, de la Directiva 95/46, al que se remite el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 (véase, en ese sentido, la sentencia de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartado 53). Dicha enumeración de objetivos tiene carácter exhaustivo, como se deriva del artículo 15, apartado 1, segunda frase, de esta última Directiva, a cuyo tenor las medidas legales deben estar justificadas por alguno de «los motivos establecidos» en el artículo 15, apartado 1, primera frase, de dicha Directiva. Por tanto, los Estados miembros no podrán adoptar tales medidas con fines distintos de los enumerados en esta última disposición.

91 Además, el artículo 15, apartado 1, tercera frase, de la Directiva 2002/58 dispone que «todas las medidas contempladas en el [artículo 15, apartado 1, de la Directiva 2002/58] deberán ser conformes con los principios generales del Derecho [de la Unión], incluidos los mencionados en los apartados 1 y 2 del artículo 6 [UE]», entre los que figuran los principios generales y los derechos fundamentales que actualmente se encuentran garantizados en la Carta. El artículo 15, apartado 1, de la Directiva 2002/58 debe, por tanto, interpretarse a la luz de los derechos fundamentales garantizados por la Carta (véanse, por analogía, por lo que se refiere a la Directiva 95/46, las sentencias de 20 de mayo de 2003, Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartado 68; de 13 de mayo de 2014, Google Spain y Google, C-131/12, EU:C:2014:317, apartado 68, y de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 38).

92 A este respecto, debe señalarse que la obligación impuesta a los proveedores de servicios de comunicaciones electrónicas, mediante una normativa nacional como la controvertida en el asunto principal, de conservar los datos de tráfico con el fin de hacerlos accesibles, en su caso, a las autoridades nacionales competentes suscita dudas en cuanto al cumplimiento no sólo de los

artículos 7 y 8 de la Carta, que se mencionan expresamente en las cuestiones prejudiciales, sino también al respeto de la libertad de expresión garantizada en el artículo 11 de la Carta (véase, por analogía, por lo que se refiere a la Directiva 2006/24, la sentencia Digital Rights, apartados 25 y 70).

93 Así, la importancia tanto del derecho al respeto de la vida privada, garantizado por el artículo 7 de la Carta, como del derecho a la protección de los datos personales, que garantiza el artículo 8 de ésta, tal como se deriva de la jurisprudencia del Tribunal de Justicia (véase, en ese sentido, la sentencia de 6 octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 39 y jurisprudencia citada), debe tomarse en consideración a la hora de interpretar el artículo 15, apartado 1, de la Directiva 2002/58. Lo mismo cabe afirmar del derecho a la libertad de expresión, habida cuenta de la especial importancia que tiene esta libertad en toda sociedad democrática. Este derecho fundamental, garantizado en el artículo 11 de la Carta, constituye uno de los fundamentos esenciales de una sociedad democrática y pluralista, y forma parte de los valores en los que se basa, con arreglo al artículo 2 TUE, la Unión (véanse, en ese sentido, las sentencias de 12 de junio de 2003, Schmidberger, C-112/00, EU:C:2003:333, apartado 79, y de 6 de septiembre de 2011, Patriciello, C-163/10, EU:C:2011:543, apartado 31).

94 A este respecto, procede recordar que, con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley y respetar su contenido esencial. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones al ejercicio de esos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás (sentencia de 15 de febrero de 2016, N., C-601/15 PPU, EU:C:2016:84, apartado 50).

95 Sobre este último extremo, el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 establece que los Estados miembros podrán adoptar una medida que suponga una excepción al principio de confidencialidad de las comunicaciones y de los datos de tráfico relativos a ellas cuando sea «necesaria, proporcionada y apropiada en una sociedad democrática», a la vista de los objetivos que enuncia dicha disposición. El considerando 11 de esta Directiva precisa, por su parte, que una medida de esta naturaleza debe ser «rigurosamente» proporcionada al objetivo que pretende lograr. Por lo que se refiere, concretamente, a la conservación de datos, el artículo 15, apartado 1, segunda frase, de dicha Directiva exige que ésta sólo se realice «durante un plazo limitado» y «justificado» por alguno de los objetivos contemplados en el artículo 15, apartado 1, primera frase, de esa misma Directiva.

96 El respeto del principio de proporcionalidad se desprende igualmente de la reiterada jurisprudencia del Tribunal de Justicia según la cual la protección del derecho fundamental al respeto de la vida privada a nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (sentencias de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 56; de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 77; Digital Rights, apartado 52, y de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 92).

97 En relación con la cuestión de si una normativa nacional como la controvertida en el asunto C-203/15 cumple esos requisitos, debe señalarse que ésta prevé una conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica, y obliga a los proveedores de servicios de comunicaciones electrónicas a conservar esos datos de manera sistemática y continuada, sin ninguna excepción. Como se desprende de la resolución de remisión, las categorías de datos a las que se refiere dicha normativa se corresponden, en esencia, con aquellas cuya conservación estaba prevista por la Directiva 2006/24.

98 Así, los datos que deben conservar los proveedores de servicios de comunicaciones electrónicas permiten rastrear e identificar el origen de una comunicación y su destino, determinar la fecha, la hora, la duración y la naturaleza de una comunicación así como el equipo de comunicación de los usuarios, y localizar el equipo de comunicación móvil. Entre esos datos se encuentra el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet. Estos datos permiten, en concreto, saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde el que se ha realizado. Además, permiten conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 26).

99 Estos datos, considerados en su conjunto, permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 27). En particular, estos datos proporcionan medios para determinar, como ha señalado el Abogado General en los puntos 253, 254 y 257 a 259 de sus conclusiones, el perfil de las personas afectadas, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones.

100 La injerencia que supone una normativa de este tipo en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta tiene una gran magnitud y debe considerarse especialmente grave. El hecho de que la conservación de los datos se efectúe sin que los usuarios de los servicios de comunicaciones electrónicas hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 37).

101 Aunque tal normativa no autorice la conservación del contenido de las comunicaciones ni pueda, por tanto, vulnerar el contenido esencial de esos derechos (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 39), la conservación de datos de tráfico y de localización podría, no obstante, influir en el uso de los medios de comunicación electrónica y, en consecuencia, en el ejercicio por los usuarios de esos medios de su libertad de expresión, garantizada por el artículo 11 de la Carta (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 28).

102 Habida cuenta de la gravedad de la injerencia en los derechos fundamentales afectados que supone una normativa nacional que prevé, a efectos de la lucha contra la delincuencia, la conservación de datos de tráfico y de localización, sólo la lucha contra la delincuentica grave puede justificar una medida de este tipo (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 60).

103 Además, si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 51).

104 A este respecto, debe señalarse, por una parte, que una normativa de este tipo tiene como consecuencia, habida cuenta de sus características, descritas en el apartado 97 de la presente sentencia, que la conservación de los datos de tráfico y de localización se convierta en la regla, mientras que el sistema creado por la Directiva 2002/58 exige que esa conservación de datos sea excepcional.

105 Por otra parte, una normativa nacional, como la controvertida en el asunto principal, que cubre de manera generalizada a todos los abonados y usuarios registrados y que tiene por objeto todos los medios de comunicación electrónica así como todos los datos de tráfico, no establece ninguna diferenciación, limitación o excepción en función del objetivo que se pretende lograr. Esta normativa afecta globalmente a todas las personas que hacen uso de servicios de comunicaciones electrónicas, aunque no se encuentren, ni siquiera indirectamente, en una situación que justifique una acción penal. Por tanto, esa normativa se aplica incluso a las personas de las que no existe ningún indicio para pensar que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves. Además, no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas a secreto profesional conforme al Derecho nacional (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartados 57 y 58).

106 Una normativa de este tipo no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública. En particular, no está limitada a una conservación de datos referentes a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 59).

107 Una normativa nacional como la controvertida en el asunto principal excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta.

108 En cambio, el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a que un Estado miembro adopte una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido.

109 Para cumplir los requisitos enumerados en el apartado anterior de la presente sentencia, dicha normativa nacional debe establecer, en primer lugar, normas claras y precisas que regulen el alcance y la aplicación de una medida de conservación de datos de este tipo y que establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a los riesgos de abuso. Debe indicar, en particular, en qué circunstancias y con arreglo a qué requisitos puede adoptarse, con carácter preventivo, una medida de conservación de datos, garantizando que tal medida se limite a lo estrictamente necesario (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 54 y jurisprudencia citada).

110 En segundo lugar, en relación con los requisitos materiales que debe cumplir una normativa nacional que permita, en el contexto de la lucha contra la delincuencia, la conservación con carácter preventivo de datos de tráfico y de localización, para garantizar que se limita a lo estrictamente necesario, debe señalarse que, si bien tales requisitos pueden variar en función de las medidas adoptadas a efectos de la prevención, investigación, descubrimiento y persecución de la delincuencia grave, la conservación de los datos debe responder en todo caso a criterios objetivos y debe existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr. En particular, tales requisitos deben permitir que pueda delimitarse en la práctica de modo efectivo el alcance de la medida y, en consecuencia, el público afectado.

111 Por lo que se refiere a la delimitación de una medida de este tipo en cuanto al público y a las situaciones potencialmente afectadas, la normativa nacional debe basarse en elementos objetivos que permitan dirigirse a un público cuyos datos puedan presentar una relación, por lo menos indirecta, con delitos graves, contribuir de un modo u otro a la lucha contra la delincuencia grave o prevenir un riesgo grave para la seguridad pública. Tal delimitación puede garantizarse mediante un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de elementos objetivos, que existe un riesgo elevado de preparación o de comisión de tales delitos en una o varias zonas geográficas.

112 Habida cuenta de las anteriores consideraciones, procede responder a la primera cuestión prejudicial en el asunto C-203/15 que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.

Sobre la segunda cuestión prejudicial en el asunto C-203/15 y la primera cuestión prejudicial en el asunto C-698/15

113 Con carácter preliminar, procede señalar que el Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo) sólo planteó la segunda cuestión prejudicial en el asunto C-203/15 en caso de respuesta negativa a la primera cuestión prejudicial en ese asunto. No obstante, esta segunda cuestión prejudicial es independiente del carácter generalizado o selectivo de una conservación de datos, en el sentido expuesto en los apartados 108 a 111 de la presente sentencia. Por tanto, procede responder conjuntamente a la segunda cuestión prejudicial en el asunto C-203/15 y a la primera cuestión prejudicial en el asunto C-698/15, que fue planteada con independencia del alcance de la obligación de conservación de datos impuesta a los proveedores de servicios de comunicaciones electrónicas.

114 Mediante la segunda cuestión prejudicial en el asunto C-203/15 y la primera cuestión prejudicial en el asunto C-698/15, los tribunales remitentes solicitan, en esencia, que se dilucide si el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso a los casos de lucha contra la delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión.

115 Respecto a los objetivos que pueden justificar una normativa nacional que establece una excepción al principio de confidencialidad de las comunicaciones electrónicas, debe recordarse que, puesto que, como se ha indicado en los apartados 90 y 102 de la presente sentencia, la enumeración de los objetivos que figuran en el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 tiene carácter exhaustivo, el acceso a los datos conservados debe responder efectiva y estrictamente a uno de esos objetivos. Además, dado que el objetivo perseguido por dicha normativa debe guardar una relación con la gravedad de la injerencia en los derechos fundamentales que supone este acceso, de ello se deriva que, en materia de prevención, investigación, descubrimiento y persecución de delitos, sólo la lucha contra la delincuencia grave puede justificar dicho acceso a los datos conservados.

116 En relación con el respeto del principio de proporcionalidad, una normativa nacional que regula los requisitos con arreglo a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos conservados debe garantizar, conforme a lo expresado en los apartados 95 y 96 de la presente sentencia, que tal acceso sólo se produzca dentro de los límites de lo estrictamente necesario.

117 Además, puesto que, conforme al considerando 11 de la Directiva 2002/58, las medidas legales a que se refiere el artículo 15, apartado 1, de ésta deben «estar sujetas [...] a salvaguardias adecuadas», una medida de este tipo debe establecer, como resulta de la jurisprudencia citada en el apartado 109 de la presente sentencia, normas claras y precisas que indiquen en qué circunstancias y con arreglo a qué requisitos los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos. Del mismo modo, una medida de esta naturaleza debe ser legalmente imperativa en Derecho interno.

118 Para garantizar que el acceso de las autoridades nacionales competentes a los datos conservados se limite a lo estrictamente necesario, es ciertamente el Derecho nacional el que debe determinar los requisitos conforme a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder dicho acceso. No obstante, la normativa nacional de que se trata no puede limitarse a exigir que el acceso responda a alguno de los objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, ni siquiera el de la lucha contra la delincuencia grave. En efecto, tal normativa nacional debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 61).

119 De este modo, y puesto que un acceso general a todos los datos conservados, con independencia de la existencia de una relación, por lo menos indirecta, con el fin perseguido, no puede considerarse limitado a lo estrictamente necesario, la normativa nacional de que se trate debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos de los abonados o usuarios registrados. A este respecto, en principio sólo podrá concederse un acceso en relación con el objetivo de la lucha contra la delincuencia a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave (véase, por analogía, TEDH, 4 de diciembre de 2015, Zakharov c. Rusia, CE:ECHR:2015:1204JUD004714306, § 260). No obstante, en situaciones particulares, como aquellas en las que intereses vitales de la seguridad nacional, la defensa o la seguridad pública están amenazados por actividades terroristas, podría igualmente concederse el acceso a los datos de otras personas cuando existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra dichas actividades.

120 Para garantizar en la práctica el pleno cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se produzca a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, descubrimiento o acciones penales (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 62; véanse igualmente, por analogía, en relación con el artículo 8 del CEDH, TEDH, 12 de enero de 2016, Szabó y Vissy c. Hungría, CE:ECHR:2016:0112JUD003713814, §§ 77 y 80).

121 Del mismo modo, es necesario que las autoridades nacionales competentes a las que se conceda el acceso a los datos conservados informen de ello a las personas afectadas, en el marco de los procedimientos nacionales aplicables, siempre que esa comunicación no pueda comprometer las investigaciones que llevan a cabo esas autoridades. En efecto, esa información es, de hecho, necesaria para que dichas personas puedan ejercer, concretamente, su derecho a la tutela judicial efectiva,

previsto expresamente en el artículo 15, apartado 2, de la Directiva 2002/58, en relación con el artículo 22 de la Directiva 95/46, en caso de vulneración de sus derechos (véanse, por analogía, las sentencias de 7 de mayo de 2009, Rijkeboer, C-553/07, EU:C:2009:293, apartado 52, y de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 95).

122 En lo que respecta a las normas relativas a la seguridad y a la protección de los datos conservados por los proveedores de servicios de comunicaciones electrónicas, debe señalarse que el artículo 15, apartado 1, de la Directiva 2002/58 no permite a los Estados miembros establecer excepciones al artículo 4, apartados 1 y 1 *bis*, de ésta. Estas últimas disposiciones exigen que los proveedores adopten medidas técnicas y de gestión adecuadas que permitan garantizar una protección eficaz de los datos conservados contra los riesgos de abuso y contra todo acceso ilícito a esos datos. Habida cuenta de la cantidad de datos conservados, del carácter sensible de esos datos y del riesgo de acceso ilícito a éstos, los proveedores de servicios de comunicaciones electrónicas deben garantizar, para asegurar la plena integridad y confidencialidad de esos datos, un nivel particularmente elevado de protección y de seguridad mediante medidas técnicas y de gestión adecuadas. En particular, la normativa nacional debe prever la conservación de los datos en el territorio de la Unión y la destrucción definitiva de los datos al término del período de conservación de éstos (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartados 66 a 68).

123 En todo caso, los Estados miembros deben garantizar el control por una autoridad independiente del respeto del nivel de protección garantizado por el Derecho de la Unión en materia de protección de las personas físicas en relación con el tratamiento de datos personales. Este control viene exigido expresamente por el artículo 8, apartado 3, de la Carta y constituye, con arreglo a reiterada jurisprudencia del Tribunal de Justicia, un elemento esencial del respeto de la protección de las personas respecto al tratamiento de datos personales. Si no fuera así, las personas cuyos datos personales han sido conservados se verían privadas del derecho, garantizado en el artículo 8, apartados 1 y 3, de la Carta, a solicitar la protección de sus datos personales ante las autoridades nacionales de control (véanse, en ese sentido, las sentencias Digital Rights, apartado 68, y de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartados 41 y 58).

124 Corresponde a los órganos jurisdiccionales remitentes verificar si, y en qué medida, las normativas nacionales de que se trata en los asuntos principales cumplen las exigencias derivadas del artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, tal y como se concretan en los apartados 115 a 123 de la presente sentencia, por lo que se refiere tanto al acceso de las autoridades nacionales competentes a los datos conservados como a la protección y el nivel de seguridad de estos datos.

125 Habida cuenta de las anteriores consideraciones, procede responder a la segunda cuestión prejudicial en el asunto C-203/15 y a la primera cuestión prejudicial en el asunto C-698/15 que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión.

Sobre la segunda cuestión prejudicial en el asunto C-698/15

126 Mediante su segunda cuestión prejudicial en el asunto C-698/15, la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil)] solicita, en esencia, que se dilucide si en la sentencia Digital Rights el Tribunal de Justicia ha interpretado los artículos 7 u 8 de la Carta en un sentido más amplio que el conferido al artículo 8 del CEDH por el Tribunal Europeo de Derechos Humanos.

127 Con carácter preliminar, debe recordarse que, si bien los derechos fundamentales reconocidos por el CEDH forman parte del Derecho de la Unión como principios generales —como confirma el artículo 6 TUE, apartado 3—, dicho Convenio no constituye, dado que la Unión no se ha adherido a él, un instrumento jurídico integrado formalmente en el ordenamiento jurídico de la Unión (véase, en ese sentido, la sentencia de 15 de febrero de 2016, N., C-601/15 PPU, EU:C:2016:84, apartado 45 y jurisprudencia citada).

128 De ese modo, la interpretación de la Directiva 2002/58, de que se trata en el presente asunto, debe basarse únicamente en los derechos fundamentales garantizados por la Carta (véase, en ese sentido, la sentencia de 15 de febrero de 2016, N., C-601/15 PPU, EU:C:2016:84, apartado 46 y jurisprudencia citada).

129 Además, procede recordar que las explicaciones relativas al artículo 52 de la Carta indican que el apartado 3 de ese artículo pretende garantizar la coherencia necesaria entre la Carta y el CEDH, «sin que ello afecte a la autonomía del Derecho de la Unión y del Tribunal de Justicia de la Unión Europea» (sentencia de 15 de febrero de 2016, N., C-601/15 PPU, EU:C:2016:84, apartado 47). En particular, como prevé expresamente el artículo 52, apartado 3, segunda frase, de la Carta, el artículo 52, apartado 3, primera frase, de ésta no impide que el Derecho de la Unión conceda una protección más amplia que el CEDH. A esto se añade, finalmente, el hecho de que el artículo 8 de la Carta se refiere a un derecho fundamental distinto del previsto en el artículo 7 de ésta y que no tiene equivalente en el CEDH.

130 Pues bien, conforme a reiterada jurisprudencia del Tribunal de Justicia, la justificación de una petición de decisión prejudicial no es la formulación de opiniones consultivas sobre cuestiones generales o hipotéticas, sino la necesidad inherente a la solución efectiva de un litigio relativo al Derecho de la Unión (véanse, en ese sentido, las sentencias de 24 de abril de 2012, Kamberaj, C-571/10, EU:C:2012:233, apartado 41; de 26 de febrero de 2013, Åkerberg Fransson, C-617/10, EU:C.2013:105, apartado 42, y de 27 de febrero de 2014, Pohotovosť, C-470/12, EU:C:2014:101, apartado 29).

131 En el presente asunto, habida cuenta de las consideraciones formuladas en los apartados 128 y 129 de la presente sentencia, la cuestión de si la protección conferida por los artículos 7 y 8 de la Carta va más allá de la garantizada en el artículo 8 del CEDH no puede influir en la interpretación de la Directiva 2002/58, a la luz de la Carta, que es objeto de controversia en el litigio principal en el asunto C-698/15

132 Así, no parece que una respuesta a la segunda cuestión prejudicial en el asunto C-698/15 pueda aportar elementos de interpretación del Derecho de la Unión necesarios para la resolución del litigio con arreglo a este Derecho.

133 En consecuencia, la segunda cuestión prejudicial en el asunto C-698/15 es inadmisible.

Costas

134 Dado que el procedimiento tiene, para las partes del litigio principal, el carácter de un incidente promovido ante los órganos jurisdiccionales nacionales, corresponde a estos 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 (Gran Sala) declara:

1) **El artículo 15, apartado 1, de la 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 Europeo y del Consejo, de 25 de noviembre de 2009, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.**

2) **El artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales, debe interpretarse en el sentido de que se opone a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión.**

3) **La segunda cuestión prejudicial planteada por la Court of Appeal (England & Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil) (Reino Unido)] es inadmisible.**

Firmas