Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 6 de octubre de 2020*

«Procedimiento prejudicial — Tratamiento de datos de carácter personal en el sector de las comunicaciones electrónicas — Proveedores de servicios de comunicaciones electrónicas — Transmisión generalizada e indiferenciada de datos de tráfico y de localización — Protección de la seguridad nacional — Directiva 2002/58/CE — Ámbito de aplicación — Artículos 1, apartado 3, y 3 — Confidencialidad de las comunicaciones electrónicas — Protección — Artículos 5 y 15, apartado 1 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8, 11 y artículo 52, apartado 1 — Artículo 4 TUE, apartado 2»

En el asunto C-623/17,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por el Investigatory Powers Tribunal (Tribunal de las Facultades de Investigación, Reino Unido), mediante resolución de 18 de octubre de 2017, recibida en el Tribunal de Justicia el 31 de octubre de 2017, en el procedimiento entre

Privacy International

y

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. K. Lenaerts, Presidente, la Sra. R. Silva de Lapuerta, Vicepresidenta, los Sres. J.-C. Bonichot y A. Arabadjiev, la Sra. A. Prechal, los Sres. M. Safjan y P. G. Xuereb y la Sra. L. S. Rossi, Presidentes de Sala, y los Sres. J. Malenovský, L. Bay Larsen y T. von Danwitz (Ponente), las Sras. C. Toader y K. Jürimäe y los Sres. C. Lycourgos y N. Piçarra, Jueces;

Abogado General: Sr. M. Campos Sánchez-Bordona;

Secretaria: Sra. C. Strömholm, administradora;

* Lengua de procedimiento: inglés.

habiendo considerado los escritos obrantes en autos y celebrada la vista los días 9 y 10 de septiembre de 2019;

consideradas las observaciones presentadas:

– en nombre de Privacy International, por los Sres. B. Jaffey y T. de la Mare, QC, por el Sr. D. Cashman, Solicitor, y por el Sr. H. Roy, avocat;

– en nombre del Gobierno del Reino Unido, por las Sras. Z. Lavery y D. Guðmundsdóttir y por el Sr. S. Brandon, en calidad de agentes, asistidos por los Sres. G. Facenna y D. Beard, QC, y los Sres. C. Knight y R. Palmer, Barristers;

– en nombre del Gobierno belga, por los Sres. P. Cottin y J.-C. Halleux, en calidad de agentes, asistidos por el Sr. J. Vanpraet, advocaat, y el Sr. E. de Lophem, avocat;

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

– en nombre del Gobierno alemán, inicialmente por los Sres. M. Hellmann, R. Kanitz, D. Klebs y T. Henze, y posteriormente por los Sres. J. Möller, M. Hellmann, R. Kanitz y D. Klebs, en calidad de agentes;

– en nombre del Gobierno estonio, por la Sra. A. Kalbus, en calidad de agente;

– en nombre del Gobierno irlandés, por las Sras. M. Browne y G. Hodge y por el Sr. A. Joyce, en calidad de agentes, asistidos por el Sr. D. Fennelly, Barrister;

– en nombre del Gobierno español, inicialmente por el Sr. L. Aguilera Ruiz y la Sra. M. J. García-Valdecasas Dorrego, y posteriormente por el Sr. L. Aguilera Ruiz, en calidad de agentes;

– en nombre del Gobierno francés, inicialmente por las Sras. E. de Moustier, E. Armoët y A.-L. Desjonquères y por los Sres. F. Alabrune, D. Colas y D. Dubois, y posteriormente por las Sras. E. de Moustier, E. Armoët y A.-L. Desjonquères y por los Sres. F. Alabrune y D. Dubois, en calidad de agentes;

– en nombre del Gobierno chipriota, por las Sras. E. Symeonidou y E. Neofytou, en calidad de agentes;

– en nombre del Gobierno letón, inicialmente por las Sras. V. Soņeca e I. Kucina, y posteriormente por la Sra. V. Soņeca, en calidad de agentes;

– en nombre del Gobierno húngaro, inicialmente por los Sres. G. Koós, M. Z. Fehér y G. Tornyai y por la Sra. Z. Wagner, y posteriormente por los Sres. G. Koós y Z. Fehér, en calidad de agentes;

– en nombre del Gobierno neerlandés, por las Sras. C. S. Schillemans y M. K. Bulterman, en calidad de agentes;

– en nombre del Gobierno polaco, por el Sr. B. Majczyna y las Sras. J. Sawicka y M. Pawlicka, en calidad de agentes;

– en nombre del Gobierno portugués, por los Sres. L. Inez Fernandes y M. Figueiredo y por la Sra. F. Aragão Homem, en calidad de agentes;

– en nombre del Gobierno sueco, inicialmente por las Sras. A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren y A. Alriksson, y posteriormente por las Sras. H. Shev, C. Meyer-Seitz, L. Zettergren y A. Alriksson, en calidad de agentes;

– en nombre del Gobierno noruego, por los Sres. T. B. Leming, M. Emberland y J. Vangsnes, en calidad de agentes;

– en nombre de la Comisión Europea, inicialmente por los Sres. H. Kranenborg, M. Wasmeier y D. Nardi y por la Sra. P. Costa de Oliveira, y posteriormente por los Sres. H. Kranenborg, M. Wasmeier y D. Nardi, en calidad de agentes;

– en nombre del Supervisor Europeo de Protección de Datos, por el Sr. T. Zerdick y la Sra. A. Buchta, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 15 de enero de 2020;

dicta la siguiente

Sentencia

1 La petición de decisión prejudicial tiene por objeto la interpretación de los artículos 1, apartado 3, y 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»), a la luz del artículo 4 TUE, apartado 2, y de los artículos 7 y 8 y del artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

2 Esta petición se ha presentado en el contexto de un litigio entre, por un lado, Privacy International y, por otro, el Secretary of State for Foreign and Commonwealth Affairs (Ministro de Asuntos Exteriores y de la Commonwealth, Reino Unido), el Secretary of State for the Home Departement (Ministro del Interior, Reino Unido), el Government Communications Headquarters (Centro Gubernamental de Comunicaciones, Reino Unido; en lo sucesivo, «GCHQ»), el Security Service (Servicio de Seguridad, Reino Unido; en lo sucesivo, «M15») y el Secret Intelligence Service (Servicio Secreto de Inteligencia, Reino Unido; en lo sucesivo, «M16»), relativo a la legalidad de una normativa que autoriza la adquisición y uso por parte de las agencias de seguridad e inteligencia de datos de comunicaciones masivos (*bulk communications data*).

Marco jurídico

Derecho de la Unión

Directiva 95/46/CE

3 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), fue derogada, con efectos a partir del 25 de mayo de 2018, por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DO 2016, L 119, p. 1). El artículo 3 de dicha Directiva, titulado «Ámbito de aplicación», tenía el siguiente tenor:

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

2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:

– efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI [TUE] y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;

– efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.»

Directiva 2002/58

4 Los considerandos 2, 6, 7, 11, 22, 26 y 30 de la Directiva 2002/58 indican lo siguiente:

«(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 [esta].

[…]

(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], la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho [de la Unión]. 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, [firmado en Roma el 4 de noviembre de 1950,] según la interpretación que se hace de este 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.

[…]

(22) Al prohibirse el almacenamiento de comunicaciones, o de los datos de tráfico relativos a estas, 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 solo 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. Cuando resulte necesario para hacer más eficaz la transmisión de toda información públicamente asequible a otros destinatarios del servicio a solicitud de los mismos, la presente Directiva no debe evitar que dicha información siga almacenada más tiempo, siempre que la misma sea, en cualquier caso, asequible al público sin restricciones y que se eliminen todos los datos relativos a los abonados o usuarios individuales que pidan tal información.

[…]

(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 estas al respeto de su correspondencia, o se refieren a los intereses legítimos de las personas jurídicas. Dichos datos solo 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 […] solo 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. Los datos sobre tráfico utilizados para la comercialización de los servicios de comunicaciones […] deben también eliminarse o hacerse anónimos tras la prestación del servicio.

[…]

(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. […]»

5 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 necesarias 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 [Unión Europea].

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 [TFUE], 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.»

6 Según el artículo 2 de esta Directiva, titulado «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:

a) "usuario": una persona física que utiliza con fines privados o comerciales un servicio de comunicaciones electrónicas disponible para el público, sin que necesariamente se haya abonado a dicho servicio;

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;

[…]».

7 El artículo 3 de la citada Directiva, titulado «Servicios afectados», dispone:

«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 [Unión], incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos.»

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, titulado «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.

3. 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. Solo 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, solo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido. 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, titulado «Aplicación de determinadas disposiciones de la Directiva [95/46]», establece en su apartado 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 [de la Unión], incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea.»

Reglamento 2016/679

12 El artículo 2 del Reglamento 2016/679 dispone:

«1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

[…]

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la […] protección frente a amenazas a la seguridad pública y su prevención.»

13 El artículo 4 de este Reglamento establece lo siguiente:

«A efectos del presente Reglamento se entenderá por:

[…]

2) “tratamiento”: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

[…]».

14 A tenor del artículo 23, apartado 1, del mismo Reglamento:

«El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros.

j) la ejecución de demandas civiles.»

15 Según el artículo 94, apartado 2, del Reglamento 2016/679:

«Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva [95/46] se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.»

Derecho del Reino Unido

16 El artículo 94 de la Telecommunications Act 1984, en su versión aplicable a los hechos del litigio principal (Ley de 1984 sobre las Telecomunicaciones; en lo sucesivo, «Ley de 1984»), titulado «Instrucciones en interés de la seguridad nacional, etc.», dispone:

«(1) El ministro podrá, previa consulta con una persona a la que se aplique el presente artículo, dar a dicha persona las instrucciones de carácter general que, a juicio del ministro, sean necesarias en interés de la seguridad nacional o de las relaciones con el Gobierno de un país o territorio situado fuera del Reino Unido.

(2) Si el ministro considera necesario proceder de ese modo en interés de la seguridad nacional o de las relaciones con el Gobierno de un país o territorio situado fuera del Reino Unido, podrá, previa consulta con una persona a la que se aplique el presente artículo, dar a dicha persona instrucciones para que (según las circunstancias del caso) realice o no realice una acción determinada especificada en las instrucciones.

(2A) El ministro solo podrá dar instrucciones con arreglo al apartado (1) o (2) si considera que el comportamiento exigido por las instrucciones es proporcionado al objetivo que se pretende conseguir mediante dicho comportamiento.

(3) La persona a la que se aplique el presente artículo deberá dar cumplimiento a todas las instrucciones que el ministro le dé en virtud del presente artículo, sin perjuicio de cualquier otra obligación que le incumba en virtud de la parte 1 o de la parte 2, capítulo 1, de la Communications Act 2003 [Ley de 2003 sobre Comunicaciones] y, en el caso de instrucciones impartidas al proveedor de una red pública de comunicaciones electrónicas, aun cuando dichas instrucciones le sean aplicables en una calidad distinta de la de proveedor de acceso a tal red.

(4) El ministro presentará a cada una de las cámaras del Parlamento una copia de todas las instrucciones impartidas en virtud del presente artículo, salvo si considera que la divulgación de dichas instrucciones es contraria a los intereses de la seguridad nacional o de las relaciones con el Gobierno de un país o territorio situado fuera del Reino Unido, o a los intereses comerciales de una persona.

(5) Ninguna persona revelará ni estará obligada por ley o de otro modo a revelar información relativa a las medidas adoptadas de conformidad con el presente artículo si el ministro le ha notificado que, a su juicio, dicha revelación sería contraria a los intereses de la seguridad nacional o de las relaciones con el Gobierno de un país o territorio situado fuera del Reino Unido, o a los intereses comerciales de otra persona.

[…]

(8) El presente artículo se aplicará a la [Office of communications (OFCOM)] y a los proveedores de redes públicas de comunicaciones electrónicas.»

17 El artículo 21, apartados 4 y 6, de la Regulation of Investigatory Powers Act 2000 (Ley de 2000 sobre la Regulación de las Facultades de Investigación; en lo sucesivo, «RIPA») dispone:

«(4) […] “datos de comunicaciones” tendrá cualquiera de los significados siguientes:

(a) cualquier dato de tráfico contenido o adjunto 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 esta sea o pueda ser transmitida;

(b) cualquier información que no incluya 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 telecomunicación;

(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.

[…]

(6) […] el concepto de "datos de tráfico", en relación con cualquier comunicación, se refiere a:

(a) cualquier dato que identifique o pretenda identificar a cualquier persona, aparato o localización hacia los cuales o desde los cuales se transmita o pueda transmitirse una comunicación;

(b) cualquier dato que identifique o seleccione, o pretenda identificar o seleccionar, el aparato por el que se transmite o puede transmitirse la comunicación;

(c) cualquier dato que comprenda señales para accionar el aparato utilizado en un sistema de comunicación con el fin de realizar la transmisión de cualquier comunicación; y

(d) cualquier dato que identifique los datos incluidos en una comunicación determinada o adjuntos a ella, u otros datos como datos incluidos en una comunicación determinada o adjuntos a ella.

[…]»

18 Los artículos 65 a 69 de la RIPA establecen las reglas relativas al funcionamiento y a las competencias del Investigatory Powers Tribunal (Tribunal de las Facultades de Investigación, Reino Unido). Con arreglo al artículo 65 de esta Ley, podrán presentarse reclamaciones ante el Investigatory Powers Tribunal (Tribunal de las Facultades de Investigación) si existen motivos para pensar que los datos han sido obtenidos de modo inapropiado.

Litigio principal y cuestiones prejudiciales

19 A principios de 2015, se hizo pública, en particular en un informe del Intelligence and Security Committee of Parliament (Comisión de Información y Seguridad del Parlamento, Reino Unido), la existencia de prácticas de recopilación y utilización de datos de comunicaciones masivos por parte de las distintas agencias de seguridad e inteligencia del Reino Unido, a saber, el GCHQ, el MI5 y el MI6. El 5 de junio de 2015, Privacy International, organización no gubernamental, interpuso una demanda ante el Investigatory Powers Tribunal (Tribunal de las Facultades de Investigación) contra el Ministro de Asuntos Exteriores y de la Commonwealth, el Ministro del Interior y las mencionadas agencias de seguridad e inteligencia, mediante la que impugnaba la legalidad de esas prácticas.

20 El órgano jurisdiccional remitente examinó la legalidad de dichas prácticas a la luz, en primer lugar, del Derecho interno y de lo dispuesto en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950 (en lo sucesivo, «CEDH»), y, en segundo lugar, del Derecho de la Unión. En una sentencia de 17 de octubre de 2016, dicho órgano jurisdiccional declaró que los demandados en el litigio principal habían reconocido que esas agencias de seguridad e inteligencia recababan y utilizaban, en el marco de sus actividades, conjuntos de datos relativos a particulares y pertenecientes a diferentes categorías (*bulk personal data*), tales como datos biográficos o de viajes, información financiera o comercial, datos de comunicaciones que podían contener datos sensibles protegidos por el secreto profesional, o incluso material periodístico. Estos datos, obtenidos por distintas vías, en su caso secretas, se cotejan y se analizan mediante tratamientos automatizados, pueden comunicarse a otras personas y autoridades, y compartirse con socios extranjeros. En este contexto, las agencias de seguridad e inteligencia utilizan también datos de comunicaciones masivos, recabados de los proveedores de redes públicas de comunicaciones electrónicas en virtud, en particular, de instrucciones ministeriales adoptadas sobre la base del artículo 94 de la Ley de 1984. El GCHQ y el MI5 actúan de este modo desde los años 2001 y 2005, respectivamente.

21 Dicho órgano jurisdiccional consideró que estas medidas de recopilación y utilización de datos eran conformes con el Derecho interno y, desde 2015, sin perjuicio de las cuestiones aún no examinadas acerca de la proporcionalidad de dichas medidas y de la transferencia de datos a terceros, con el

artículo 8 del CEDH. A este último respecto, señaló que se le habían presentado pruebas relativas a las garantías aplicables, en particular por lo que respecta a los procedimientos de acceso y de divulgación fuera de las agencias de seguridad e inteligencia, las modalidades de conservación de los datos y la existencia de controles independientes.

22 En lo que atañe a la legalidad de las medidas de recopilación y utilización controvertidas en el litigio principal a la luz del Derecho de la Unión, el órgano jurisdiccional remitente examinó, en una sentencia de 8 de septiembre de 2017, si tales medidas estaban comprendidas en el ámbito de aplicación de ese Derecho y, de ser así, si eran compatibles con ese Derecho. Dicho órgano jurisdiccional declaró, en relación con los datos de comunicaciones masivos, que los proveedores de redes de comunicaciones electrónicas estaban obligados, en virtud del artículo 94 de la Ley de 1984, en el supuesto de que un ministro cursara instrucciones en este sentido, a facilitar a las agencias de seguridad e inteligencia los datos recabados en el contexto de su actividad económica comprendida en el ámbito de aplicación del Derecho de la Unión. En cambio, no sucedía así en el caso de la recopilación de otros datos obtenidos por dichas agencias sin recurrir a tales facultades vinculantes. Sobre la base de esta constatación, el órgano jurisdiccional remitente consideró necesario plantear una serie de cuestiones prejudiciales al Tribunal de Justicia para determinar si un régimen como el que resulta de dicho artículo 94 está comprendido en el ámbito del Derecho de la Unión y, en caso afirmativo, si se aplican, y de qué modo, a dicho régimen los requisitos establecidos por la jurisprudencia derivada de la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, en lo sucesivo, «sentencia Tele2», EU:C:2016:970).

23 A este respecto, en su petición de decisión prejudicial, el órgano jurisdiccional remitente indica que, según el citado artículo 94, un ministro puede dar a los proveedores de servicios de comunicaciones electrónicas las instrucciones generales o específicas que considere necesarias en interés de la seguridad nacional o de las relaciones con un Gobierno extranjero. Remitiéndose a las definiciones que figuran en el artículo 21, apartados 4 y 6, de la RIPA, dicho órgano jurisdiccional señala que los datos de que se trata incluyen los datos de tráfico y la información sobre los servicios utilizados, en el sentido de esta última disposición, de manera que solo está excluido el contenido de las comunicaciones. Estos datos y esta información permiten, en particular, conocer el «quién, cuándo y cómo» de una comunicación. Dichos datos se transmiten a las agencias de seguridad e inteligencia, que los conservan para los fines de su actividad.

24 Según dicho órgano jurisdiccional, el régimen controvertido en el litigio principal se distingue del resultante de la Data Retention and Investigatory Powers Act 2014 (Ley de 2014 sobre Conservación de Datos y Facultades de Investigación), objeto del asunto que dio lugar a la sentencia de 21 de diciembre de 2016, Tele2 (C-203/15 y C-698/15, EU:C:2016:970), ya que este último régimen establecía la conservación de los datos por parte de los proveedores de servicios de comunicaciones electrónicas y su puesta a disposición no solo de las agencias de seguridad e inteligencia, en interés de la seguridad nacional, sino también de otras autoridades públicas, en función de sus necesidades. Por otra parte, dicha sentencia se refería a una investigación penal y no a la seguridad nacional.

25 El órgano jurisdiccional remitente añade que las bases de datos constituidas por las agencias de seguridad e inteligencia son objeto de un tratamiento masivo y automatizado, no específico, con el fin de detectar posibles amenazas desconocidas. A tal efecto, dicho órgano jurisdiccional señala que los conjuntos de metadatos constituidos de este modo deben ser tan exhaustivos como sea posible, para poder disponer de un «pajar» en el que encontrar «la aguja» que se oculta en él. En cuanto a la utilidad de la recopilación de datos masivos por dichas agencias y de las técnicas de consulta de estos datos, dicho órgano jurisdiccional se refiere, en particular, a las conclusiones del informe elaborado el 19 de agosto de 2016 por el Sr. David Anderson, QC, entonces United Kingdom Independent Reviewer of Terrorism Legislation (supervisor independiente del Reino Unido de la legislación sobre terrorismo), quien, para elaborar ese informe, se basó en un examen realizado por un equipo de especialistas de la información y en el testimonio de agentes de las agencias de seguridad e inteligencia.

26 El órgano jurisdiccional remitente señala asimismo que, según Privacy International, el régimen controvertido en el litigio principal es ilegal a la luz del Derecho de la Unión, mientras que los demandados en el litigio principal consideran que la obligación de transmisión de datos prevista por ese régimen, el acceso a esos datos y su utilización no están comprendidos en el ámbito de las competencias de la Unión, de conformidad, en particular, con el artículo 4 TUE, apartado 2, según el cual la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro.

27 A este respecto, el órgano jurisdiccional remitente considera, sobre la base de la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión (C-317/04 y C-318/04, EU:C:2006:346), apartados 56 a 59, relativa a la transferencia de los datos de los expedientes de los pasajeros (Passenger Name Records) con fines de protección de la seguridad pública, que las actividades de las sociedades mercantiles en el marco del tratamiento y de la transferencia de datos con el fin de proteger la seguridad nacional no parecen estar comprendidas en el ámbito de aplicación del Derecho de la Unión. A su juicio, no procede examinar si la actividad en cuestión constituye un tratamiento de datos, sino únicamente si, en su esencia y efectos, el objeto de esa actividad es apoyar una función esencial del Estado, en el sentido del artículo 4 TUE, apartado 2, a través de un marco establecido por las autoridades públicas en materia de seguridad pública.

28 En el supuesto de que las medidas controvertidas en el litigio principal estuvieran, no obstante, comprendidas en el ámbito de aplicación del Derecho de la Unión, el órgano jurisdiccional remitente considera que los requisitos establecidos en los apartados 119 a 125 de la sentencia de 21 de diciembre de 2016, Tele2 (C-203/15 y C-698/15, EU:C:2016:970), parecen inadecuados en el contexto de la seguridad nacional y podrían obstaculizar la capacidad de las agencias de seguridad e inteligencia para controlar determinadas amenazas para la seguridad nacional.

29 En este contexto, el Investigatory Powers Tribunal (Tribunal de las Facultades de Investigación) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«En circunstancias en las que:

a) la capacidad [de las agencias de seguridad e inteligencia] para usar determinados [datos de comunicaciones masivos] que se les han suministrado es esencial para proteger la seguridad nacional del Reino Unido, en particular, en los ámbitos de lucha contra el terrorismo, el espionaje y la proliferación nuclear;

b) un objetivo esencial del uso que las [agencias de seguridad e inteligencia] hacen de [los datos de comunicaciones masivos] consiste en descubrir amenazas hasta entonces desconocidas para la seguridad nacional, mediante técnicas masivas generales basadas en la acumulación de los datos de comunicaciones masivos en un único lugar. Su utilidad principal reside en la identificación y el desarrollo de objetivos de forma ágil y en la obtención de una base de actuación en caso de amenaza inminente;

c) no se exige a los proveedores de redes de comunicaciones electrónicas que conserven los [datos de comunicaciones masivos] (más allá de los plazos obligatorios), que quedan exclusivamente en poder del Estado (las [agencias de seguridad e inteligencia]);

d) el órgano jurisdiccional nacional considera que (sin perjuicio de determinadas cuestiones reservadas) las salvaguardias que rodean el uso de [los datos de comunicaciones masivos] por las [agencias de seguridad e inteligencia] cumplen los requisitos establecidos en el CEDH; y

e) el órgano jurisdiccional nacional estima que la imposición de los requisitos precisados en los apartados 119 a 125 de la sentencia [de 21 de diciembre de 2016, Tele2 (C-203/15 y C-698/15, EU:C:2016:970)], en caso de ser aplicables, redundaría en perjuicio de las medidas adoptadas por las agencias de seguridad e inteligencia para salvaguardar la seguridad nacional y, en consecuencia, pondría en riesgo la seguridad nacional del Reino Unido;

1) A la luz del artículo 4 TUE y del artículo 1, apartado 3, de la Directiva [2002/58], ¿tiene cabida en el Derecho de la Unión y en la Directiva [2002/58] un requisito por el cual un proveedor de redes de comunicación electrónica debe facilitar datos de comunicaciones masivos a las agencias de seguridad e inteligencia de un Estado miembro de acuerdo con las instrucciones recibidas del ministro?

2) En caso de respuesta afirmativa a la primera cuestión, ¿se aplican los requisitos [aplicables a los datos de comunicaciones conservados, indicados en los apartados 119 a 125 de la sentencia de 21 de diciembre de 2016, Tele2 (C-203/15 y C-698/15, EU:C:2016:970)] u otros requisitos, además de los impuestos por el CEDH, a las referidas instrucciones del ministro? En caso afirmativo, ¿cómo y en qué medida deben aplicarse dichos requisitos, habida cuenta de la necesidad esencial de las [agencias de seguridad e inteligencia] de usar las técnicas de adquisición masiva y tratamiento automatizado para proteger la seguridad nacional, y de la circunstancia de que tal capacidad, en caso de ser conforme con el CEDH, puede sufrir un menoscabo significativo como consecuencia de esos requisitos?»

Sobre las cuestiones prejudiciales

Sobre la primera cuestión prejudicial

30 Mediante su primera cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si el artículo 1, apartado 3, de la Directiva 2002/58, a la luz del artículo 4 TUE, apartado 2, debe interpretarse en el sentido de que está comprendida en el ámbito de aplicación de esta Directiva una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a transmitir a las agencias de seguridad e inteligencia datos de tráfico y de localización con el fin de proteger la seguridad nacional.

31 A este respecto, Privacy International alega, en esencia, que, teniendo en cuenta la doctrina derivada de la jurisprudencia del Tribunal de Justicia en cuanto al ámbito de aplicación de la Directiva 2002/58, tanto la recopilación por parte de las agencias de seguridad e inteligencia de los datos proporcionados por dichos proveedores, en virtud del artículo 94 de la Ley de 1984, como la utilización de los datos por esas agencias están comprendidas en el ámbito de aplicación de la Directiva, con independencia de que dichos datos se recopilen mediante una transmisión efectuada en tiempo diferido o en tiempo real. En particular, sostiene que el hecho de que el objetivo de protección de la seguridad nacional se enumere expresamente en el artículo 15, apartado 1, de la citada Directiva no supone que esta no sea aplicable a tales situaciones, y que el artículo 4 TUE, apartado 2, no afecta a esta apreciación.

32 En cambio, los Gobiernos del Reino Unido, checo y estonio, Irlanda y los Gobiernos francés, chipriota, húngaro, polaco y sueco alegan, en esencia, que la Directiva 2002/58 no es aplicable a la normativa nacional controvertida en el litigio principal porque esta normativa tiene como finalidad la protección de la seguridad nacional. En su opinión, las actividades de las agencias de seguridad e inteligencia son funciones esenciales de los Estados miembros relativas al mantenimiento del orden público y a la salvaguardia de la seguridad interior y de la integridad territorial, y, en consecuencia, son competencia exclusiva de estos, como pone de manifiesto, en particular, el artículo 4 TUE, apartado 2, tercera frase.

33 Según dichos Gobiernos, la Directiva 2002/58 no puede, por tanto, interpretarse en el sentido de que medidas nacionales de protección de la seguridad nacional estén comprendidas en su ámbito de aplicación. A su entender, el artículo 1, apartado 3, de esta Directiva delimita ese ámbito de aplicación y excluye de este, como ya lo hacía el artículo 3, apartado 2, primer guion, de la Directiva 95/46, las actividades relativas a la seguridad pública, la defensa y la seguridad del Estado. Consideran que estas disposiciones reflejan el reparto de competencias previsto en el artículo 4 TUE, apartado 2, y quedarían privadas de eficacia si las medidas comprendidas en el ámbito de la seguridad nacional tuvieran que respetar los requisitos de la Directiva 2002/58. Por otra parte, afirman que la jurisprudencia del Tribunal de Justicia derivada de la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión (C-317/04 y C-318/04, EU:C:2006:346), relativa al artículo 3, apartado 2, primer guion, de la Directiva 95/46, es aplicable al artículo 1, apartado 3, de la Directiva 2002/58.

34 A este respecto, ha de señalarse que, 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.

35 El artículo 1, apartado 3, de esta Directiva excluye de su ámbito de aplicación las «actividades del Estado» en los sectores que enumera, entre las que figuran las actividades en materia penal y las que tengan por objeto 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. Las actividades enumeradas en dicho apartado a título de ejemplo son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares (sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 32 y jurisprudencia citada).

36 Además, el artículo 3 de la Directiva 2002/58 dispone 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 lo tanto, debe considerarse que dicha Directiva regula las actividades de los proveedores de tales servicios (sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 33 y jurisprudencia citada).

37 En este marco, el artículo 15, apartado 1, de la Directiva 2002/58 autoriza a los Estados miembros a adoptar, cumpliendo los requisitos que prescribe, «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» (sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 71).

38 Pues bien, el artículo 15, apartado 1, de la Directiva 2002/58 presupone necesariamente que las medidas legislativas nacionales a las que se refiere estén incluidas en el ámbito de aplicación de la citada Directiva, ya que esta solo autoriza expresamente a los Estados miembros a adoptarlas cuando se cumplan los requisitos establecidos en ella. Además, tales medidas regulan, a los efectos mencionados en dicha disposición, la actividad de los proveedores de servicios de comunicaciones electrónicas (sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 34 y jurisprudencia citada).

39 Basándose principalmente en estas consideraciones, el Tribunal de Justicia ha declarado que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con su artículo 3, debe interpretarse en el sentido de que están incluidas en el ámbito de aplicación de esta Directiva no solo una medida legislativa que obliga a los proveedores de servicios de comunicaciones electrónicas a conservar los

datos de tráfico y de localización, sino también una medida legislativa que les obliga a permitir a las autoridades nacionales competentes el acceso a estos datos. En efecto, tales medidas legislativas implican necesariamente un tratamiento de los datos por esos proveedores y, en la medida en que regulan las actividades de dichos proveedores, no pueden asimilarse a actividades propias de los Estados, mencionadas en el artículo 1, apartado 3, de dicha Directiva (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartados 35 y 37 y jurisprudencia citada).

40 Por lo que se refiere a una medida legislativa como el artículo 94 de la Ley de 1984, en la que la autoridad competente puede basarse para dar a los proveedores de servicios de comunicaciones electrónicas instrucciones de que comuniquen, mediante transmisión, datos masivos a las agencias de seguridad e inteligencia, procede señalar que, en virtud de la definición que figura en el artículo 4, apartado 2, del Reglamento 2016/679, la cual es aplicable, de conformidad con el artículo 2 de la Directiva 2002/58, en relación con el artículo 94, apartado 2, de dicho Reglamento, el concepto de «tratamiento de datos personales» designa «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, […], conservación, […], consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso […]».

41 De ello se deduce que una comunicación de datos personales por transmisión constituye, al igual que una conservación de datos o cualquier otra forma de puesta a disposición, un tratamiento en el sentido del artículo 3 de la Directiva 2002/58 y, en consecuencia, está comprendida en el ámbito de aplicación de esta Directiva (véase, en este sentido, la sentencia de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartado 45).

42 Además, habida cuenta de las consideraciones que figuran en el apartado 38 de la presente sentencia y del sistema general de la Directiva 2002/58, una interpretación de esta Directiva según la cual las medidas legales contempladas en su artículo 15, apartado 1, están excluidas del ámbito de aplicación de dicha Directiva, debido a que las finalidades a las que deben responder esas medidas coinciden sustancialmente con las finalidades que persiguen las actividades mencionadas en el artículo 1, apartado 3, de la misma Directiva, privaría a dicho artículo 15, apartado 1, de toda eficacia (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 72 y 73).

43 Por tanto, como señaló en esencia el Abogado General en el punto 75 de sus conclusiones presentadas en los asuntos acumulados La Quadrature du Net y otros (C-511/18 y C-512/18, EU:C:2020:6), a las que se remite en el punto 24 de sus conclusiones presentadas en el presente asunto, el concepto de «actividades» que figura en el artículo 1, apartado 3, de la Directiva 2002/58 no puede interpretarse en el sentido de que comprende las medidas legales contempladas en el artículo 15, apartado 1, de dicha Directiva.

44 Las disposiciones del artículo 4 TUE, apartado 2, a las que se han referido los Gobiernos mencionados en el apartado 32 de la presente sentencia, no pueden desvirtuar esta conclusión. En efecto, según reiterada jurisprudencia del Tribunal de Justicia, si bien corresponde a los Estados miembros determinar sus intereses esenciales de seguridad y adoptar las medidas adecuadas para garantizar su seguridad interior y exterior, el mero hecho de que se haya adoptado una medida nacional con el fin de proteger la seguridad nacional no puede dar lugar a la inaplicabilidad del Derecho de la Unión ni dispensar a los Estados miembros de la necesaria observancia de dicho Derecho [véanse, en este sentido, las sentencias de 4 de junio de 2013, ZZ, C-300/11, EU:C:2013:363, apartado 38 y jurisprudencia citada; de 20 de marzo de 2018, Comisión/Austria (Imprenta del Estado), C-187/16, EU:C:2018:194, apartados 75 y 76, y de 2 de abril de 2020, Comisión/Polonia, Hungría y República Checa (Mecanismo temporal de reubicación de solicitantes de protección internacional), C-715/17, C-718/17 y C-719/17, EU:C:2020:257, apartados 143 y 170].

45 Es cierto que, en la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión (C-317/04 y C-318/04, EU:C:2006:346), apartados 56 a 59, el Tribunal de Justicia declaró que la transmisión de datos personales por parte de compañías aéreas a autoridades públicas de un Estado tercero con fines de prevención y de lucha contra el terrorismo y otros delitos graves no está comprendida, en virtud del artículo 3, apartado 2, primer guion, de la Directiva 95/46, en el ámbito de aplicación de esta Directiva, ya que esta transmisión se inserta en un marco creado por los poderes públicos cuyo objeto es la seguridad pública.

46 Sin embargo, en vista de las consideraciones expuestas en los apartados 36, 38 y 39 de la presente sentencia, esta jurisprudencia no puede aplicarse a la interpretación del artículo 1, apartado 3, de la Directiva 2002/58. En efecto, como ha señalado, en esencia, el Abogado General en los puntos 70 a 72 de sus conclusiones presentadas en los asuntos acumulados La Quadrature du Net y otros (C-511/18 y C-512/18, EU:C:2020:6), el artículo 3, apartado 2, primer guion, de la Directiva 95/46, al que se refiere dicha jurisprudencia, excluía del ámbito de aplicación de esta última Directiva, de manera general, el «tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado», sin distinguir en función del autor del tratamiento de datos. En cambio, en la interpretación del artículo 1, apartado 3, de la Directiva 2002/58, esta distinción resulta necesaria. En efecto, como se desprende de los apartados 37 a 39 y 42 de la presente sentencia, el conjunto de tratamientos de datos personales efectuados por los proveedores de servicios de comunicaciones electrónicas está comprendido en el ámbito de aplicación de dicha Directiva, incluidos los tratamientos que se derivan de las obligaciones que les imponen los poderes públicos, mientras que estos últimos tratamientos podían, en su caso, estar comprendidos en el ámbito de aplicación de la excepción prevista en el artículo 3, apartado 2, primer guion, de la Directiva 95/46, dada la formulación más amplia de dicha disposición, referida a todos los tratamientos de datos personales que tengan por objeto la seguridad pública, la defensa o la seguridad del Estado, con independencia de quién sea su autor.

47 Por otra parte, procede señalar que la Directiva 95/46, de la que se trataba en el asunto que dio lugar a la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión (C-317/04 y C-318/04, EU:C:2006:346), fue derogada y sustituida por el Reglamento 2016/679, con efectos a partir del 25 de mayo de 2018, en virtud del artículo 94, apartado 1, de dicho Reglamento. Pues bien, aunque este Reglamento precisa, en su artículo 2, apartado 2, letra d), que no se aplica a los tratamientos «por parte de las autoridades competentes» con fines, en particular, de prevención y detección de infracciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención, del artículo 23, apartado 1, letras d) y h), del mismo Reglamento se desprende que los tratamientos de datos personales efectuados con estos mismos fines por particulares están comprendidos en el ámbito de aplicación de este. De ello se deduce que la interpretación que precede de los artículos 1, apartado 3, 3 y 15, apartado 1, de la Directiva 2002/58 es coherente con la delimitación del ámbito de aplicación del Reglamento 2016/679, que esta Directiva completa y precisa.

48 En cambio, cuando los Estados miembros aplican directamente medidas que suponen excepciones a la confidencialidad de las comunicaciones electrónicas, sin imponer obligaciones de tratamiento a los proveedores de servicios de tales comunicaciones, la protección de los datos de las personas afectadas no está regulada por la Directiva 2002/58, sino únicamente por el Derecho nacional, sin perjuicio de la aplicación de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89), de modo que las medidas en cuestión deben cumplir en particular el Derecho nacional de rango constitucional y las exigencias del CEDH.

49 Habida cuenta de las consideraciones anteriores, procede responder a la primera cuestión prejudicial que los artículos 1, apartado 3, 3 y 15, apartado 1, de la Directiva 2002/58, a la luz del artículo 4 TUE, apartado 2, deben interpretarse en el sentido de que está comprendida en el ámbito de aplicación de

esta Directiva una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a transmitir a las agencias de seguridad e inteligencia datos de tráfico y de localización con el fin de proteger la seguridad nacional.

Sobre la segunda cuestión prejudicial

50 Mediante su segunda cuestión prejudicial, el órgano jurisdiccional remitente desea saber, en esencia, si el artículo 15, apartado 1, de la Directiva 2002/58, a la luz del artículo 4 TUE, apartado 2, y de los artículos 7, 8, 11 y del artículo 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una transmisión generalizada e indiferenciada de datos de tráfico y de localización a las agencias de seguridad e inteligencia con el fin de proteger la seguridad nacional.

51 Con carácter preliminar, procede recordar que, según las indicaciones que figuran en la petición de decisión prejudicial, el artículo 94 de la Ley de 1984 autoriza al ministro a obligar a los proveedores de servicios de comunicaciones electrónicas, mediante las instrucciones oportunas cuando lo considere necesario en interés de la seguridad nacional o de las relaciones con un Gobierno extranjero, a que transmitan a las agencias de seguridad e inteligencia los datos de comunicaciones masivos, datos que incluyen los datos de tráfico y de localización, así como información sobre los servicios utilizados, en el sentido del artículo 21, apartados 4 y 6, de la RIPA. Esta última disposición abarca, entre otros, los datos necesarios para identificar el origen y el destino de una comunicación, determinar la fecha, hora, duración y tipo de comunicación, identificar el material utilizado y localizar los equipos terminales y las comunicaciones. Entre estos datos figuran, en particular, el nombre y la dirección del usuario, el número de teléfono de la persona que realiza la llamada y el número al que ha llamado, las direcciones IP de la fuente y del destinatario de la comunicación, y las direcciones de los sitios de Internet visitados.

52 Esta comunicación mediante transmisión de datos afecta a todos los usuarios de los medios de comunicaciones electrónicas, sin que se precise si dicha transmisión debe producirse en tiempo real o de manera diferida. Según se indica en la petición de decisión prejudicial, una vez transmitidos, estos datos son conservados por las agencias de seguridad e inteligencia y permanecen a disposición de estas para los fines de su actividad, del mismo modo que las demás bases de datos que poseen dichas agencias. En particular, los datos así recabados, que se someten a tratamientos y análisis masivos automatizados, pueden cotejarse con otras bases de datos que incluyan distintas categorías de datos personales masivos o comunicarse fuera de dichas agencias y a terceros Estados. Por último, estas operaciones no están supeditadas a la autorización previa de un tribunal o de una autoridad administrativa independiente y no se notifican de ningún modo a los interesados.

53 La Directiva 2002/58 tiene como objetivo, como se desprende en particular de sus considerandos 6 y 7, proteger a los usuarios de los servicios de comunicaciones electrónicas frente a los riesgos que suponen para sus datos personales y su intimidad las nuevas tecnologías y, en especial, la creciente capacidad de almacenamiento y tratamiento informático de datos. En particular, dicha Directiva pretende, como indica su considerando 2, garantizar el pleno respeto de los derechos enunciados 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], que dio lugar a la Directiva 2002/58, se desprende que el legislador de la Unión pretendió 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».

54 A tal efecto, el artículo 5, apartado 1, de la Directiva 2002/58 dispone que «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». Esta misma disposición señala también que, «en particular, [los Estados miembros] 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» y precisa que «[este] apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad».

55 Así pues, este artículo 5, apartado 1, consagra el principio de confidencialidad tanto de las comunicaciones electrónicas como de los datos de tráfico asociados a ellas e implica, en particular, la prohibición, en principio, de que cualquier persona distinta de los usuarios almacene esas comunicaciones y datos sin el consentimiento de estos. Dado el carácter general de su tenor, esta disposición abarca necesariamente cualquier operación que permita a terceros conocer las comunicaciones y los datos relativos a ellas con fines distintos de la conducción de una comunicación.

56 La prohibición de intervenir las comunicaciones y los datos relativos a ellas que figura en el artículo 5, apartado 1, de la Directiva 2002/58 incluye, por tanto, cualquier forma de puesta a disposición de datos de tráfico y de localización por parte de los proveedores de servicios de comunicaciones electrónicas a autoridades públicas, como las agencias de seguridad e inteligencia, así como la conservación de los datos por esas autoridades, con independencia de la utilización posterior que se haga de ellos.

57 Así pues, al adoptar esta Directiva, el legislador de la Unión concretó los derechos consagrados en los artículos 7 y 8 de la Carta, de modo que los usuarios de los medios de comunicaciones electrónicas tienen derecho a contar con que, en principio, de no mediar su consentimiento, sus comunicaciones y los datos relativos a ellas permanezcan anónimos y no puedan registrarse (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 109).

58 Sin embargo, 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 dicha Directiva, de garantizar la confidencialidad de los datos personales y a las obligaciones correspondientes, mencionadas en particular en los artículos 6 y 9 de dicha Directiva, cuando tal limitación constituya una medida necesaria, apropiada y proporcionada en una sociedad democrática para proteger la seguridad nacional, la defensa y la seguridad pública, o para la prevención, investigación, descubrimiento y persecución de delitos o de la utilización no autorizada del sistema de comunicaciones electrónicas. 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 uno de esos motivos.

59 Dicho esto, la facultad de establecer excepciones a los derechos y obligaciones previstos en los artículos 5, 6 y 9 de la Directiva 2002/58 no puede justificar que la excepción a la obligación de principio de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos relativos a ellas y, en particular, a la prohibición de almacenar esos datos, establecida expresamente en el artículo 5 de dicha Directiva, se convierta en la regla (véanse, en este sentido, las sentencias de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 89 y 104, y de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 111).

60 Además, del artículo 15, apartado 1, tercera frase, de la Directiva 2002/58 se desprende que los Estados miembros solo pueden adoptar medidas legales para limitar el alcance de los derechos y obligaciones contemplados en los artículos 5, 6 y 9 de dicha Directiva que sean conformes con los principios generales del Derecho de la Unión, que sean conformes con los principios generales del Derecho de la

Unión, entre los que figura el principio de proporcionalidad, y con los derechos fundamentales garantizados por la Carta. A este respecto, el Tribunal de Justicia ya ha declarado que la obligación impuesta por un Estado miembro a los proveedores de servicios de comunicaciones electrónicas, mediante una normativa nacional, de conservar los datos de tráfico con el fin de hacerlos accesibles, en su caso, a las autoridades nacionales competentes suscita cuestiones en cuanto al cumplimiento no solo de los artículos 7 y 8 de la Carta, relativos al respeto de la vida privada y a la protección de los datos de carácter personal, respectivamente, sino también del artículo 11 de la Carta, relativo a la libertad de expresión (véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 25 y 70, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 91 y 92 y jurisprudencia citada).

61 Las mismas cuestiones se plantean también para otros tipos de tratamiento de datos, como su transmisión a personas distintas de los usuarios o el acceso a esos datos para su utilización [véase, por analogía, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 122 y 123 y jurisprudencia citada].

62 Así pues, la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 debe tener en cuenta 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 esta, tal como se deriva de la jurisprudencia del Tribunal de Justicia, y del derecho a la libertad de expresión, derecho fundamental, garantizado en el artículo 11 de la Carta, que constituye uno de los fundamentos esenciales de una sociedad democrática y pluralista, y forma parte de los valores en los que se basa la Unión, con arreglo al artículo 2 TUE (véanse, en este sentido, las sentencias de 6 de marzo de 2001, Connolly/Comisión, C-274/99 P, EU:C:2001:127, apartado 39, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 93 y jurisprudencia citada).

63 No obstante, los derechos consagrados en los artículos 7, 8 y 11 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse según su función en la sociedad (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 172 y jurisprudencia citada).

64 En efecto, como se desprende del artículo 52, apartado 1, de la Carta, esta admite limitaciones del ejercicio de estos derechos, siempre que esas limitaciones sean establecidas por la ley, respeten el contenido esencial de esos derechos y, dentro del respeto del principio de proporcionalidad, 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.

65 Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

66 En lo que respecta al respeto del principio de proporcionalidad, el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 dispone 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 esa medida 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 que una medida de esta naturaleza debe ser «rigurosamente» proporcionada al objetivo que pretende lograr.

67 A este respecto, debe recordarse que la protección del derecho fundamental a la intimidad exige, conforme a la jurisprudencia reiterada del Tribunal de Justicia, que las excepciones a la protección de los datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de lo

estrictamente necesario. Además, no puede perseguirse un objetivo de interés general sin tener en cuenta que debe conciliarse con los derechos fundamentales afectados por la medida, y debe efectuarse una ponderación equilibrada entre el objetivo y los intereses y derechos de que se trate [véanse, en este sentido, las 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, apartados 76, 77 y 86, y de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 52; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 140].

68 Para cumplir el requisito de proporcionalidad, una normativa debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger de manera eficaz esos datos frente a los riesgos de abuso. Dicha normativa debe ser legalmente imperativa en Derecho interno y, en particular, indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automatizado, sobre todo cuando existe un riesgo elevado de acceso ilícito a ellos. Estas consideraciones son aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles [véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].

69 En cuanto a la cuestión de si una normativa nacional como la controvertida en el litigio principal cumple los requisitos del artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y con el artículo 52, apartado 1, de la Carta, procede señalar que la transmisión de datos de tráfico y de localización a personas distintas de los usuarios, tales como las agencias de seguridad e inteligencia, constituye una excepción al principio de confidencialidad. Cuando esta operación se efectúa, como en el caso de autos, de manera generalizada e indiferenciada, produce el efecto de que la excepción a la obligación de principio de garantizar la confidencialidad de los datos se convierte en la regla, mientras que el sistema previsto por la Directiva 2002/58 exige que esa excepción siga siendo la excepción.

70 Además, según reiterada jurisprudencia del Tribunal de Justicia, la transmisión de los datos de tráfico y de localización a un tercero constituye una injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, con independencia de la utilización posterior que se haga de esos datos. A este respecto, carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia [véanse, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126 y jurisprudencia citada, y la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 115 y 116].

71 La injerencia que supone la transmisión de los datos de tráfico y de localización a las agencias de seguridad e inteligencia en el derecho consagrado en el artículo 7 de la Carta debe considerarse especialmente grave, habida cuenta, en particular, del carácter sensible de la información que pueden proporcionar esos datos y, en particular, de la posibilidad de determinar a partir de ellos el perfil de las personas afectadas, ya que tal información es tan sensible como el propio contenido de las comunicaciones. Además, puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante (véanse, por analogía, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 27 y 37, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 99 y 100).

72 Ha de señalarse, además, que la transmisión de datos de tráfico y de localización a autoridades públicas con fines de seguridad puede vulnerar en sí misma el derecho al respeto de las comunicaciones, consagrado en el artículo 7 de la Carta, y provocar efectos disuasorios en el ejercicio por los usuarios de los medios de comunicaciones electrónicas de su libertad de expresión, garantizada en el artículo 11 de la Carta. Tales efectos disuasorios pueden repercutir, en particular, en las personas cuyas comunicaciones estén sujetas, según las normas nacionales, al secreto profesional y en los denunciantes cuyas actividades estén protegidas por la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (DO 2019, L 305, p. 17). Además, estos efectos son tanto más graves cuanto más elevada sea la cantidad y la variedad de datos conservados (véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 28; de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 101, y de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 118).

73 Por último, en vista de la gran cantidad de datos de tráfico y de localización que pueden conservarse de manera continua mediante una medida de conservación generalizada y del carácter sensible de la información que esos datos pueden proporcionar, su mera conservación por parte de los proveedores de servicios de comunicaciones electrónicas conlleva riesgos de abuso y de acceso ilícito.

74 Por lo que respecta a los objetivos que pueden justificar tales injerencias, más concretamente al objetivo de protección de la seguridad nacional controvertido en el litigio principal, debe señalarse, para empezar, que el artículo 4 TUE, apartado 2, establece que la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro. Esta responsabilidad corresponde al interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad e incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país, en particular las actividades que puedan amenazar directamente a la sociedad, a la población o al propio Estado, como las actividades terroristas (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 135).

75 Pues bien, la importancia del objetivo de protección de la seguridad nacional, interpretado a la luz del artículo 4 TUE, apartado 2, supera la de los demás objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, en particular los objetivos de lucha contra la delincuencia en general, incluso grave, y de protección de la seguridad pública. En efecto, amenazas como las mencionadas en el apartado anterior se distinguen, por su naturaleza y especial gravedad, del riesgo general de que surjan tensiones o perturbaciones, incluso graves, que afecten a la seguridad pública. Por lo tanto, sin perjuicio del cumplimiento de los demás requisitos establecidos en el artículo 52, apartado 1, de la Carta, el objetivo de protección de la seguridad nacional puede justificar medidas que supongan injerencias en los derechos fundamentales más graves que las que podrían justificar esos otros objetivos (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 136).

76 No obstante, para cumplir el requisito de proporcionalidad recordado en el apartado 67 de la presente sentencia, según el cual las excepciones a la protección de los datos personales y las limitaciones de esta deben establecerse sin sobrepasar los límites de lo estrictamente necesario, una normativa nacional que suponga una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta debe respetar los requisitos derivados de la jurisprudencia citada en los apartados 65, 67 y 68 de la presente sentencia.

77 En particular, por lo que se refiere al acceso de una autoridad a datos personales, una normativa no puede limitarse a exigir que el acceso de las autoridades a los datos responda a la finalidad perseguida por dicha normativa, sino que también debe establecer los requisitos materiales y procedimentales que regulen dicha utilización [véase, por analogía, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 192 y jurisprudencia citada].

78 De este modo, y puesto que un acceso general a todos los datos conservados, sin que exista una relación, aunque sea indirecta, con el fin perseguido, no puede considerarse limitado a lo estrictamente necesario, una normativa nacional que regule el acceso a los datos de tráfico y de localización 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 que se trate (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 119 y jurisprudencia citada).

79 Estas exigencias se aplican, con mayor razón, a una medida legal, como la controvertida en el litigio principal, en la que la autoridad nacional competente puede basarse para obligar a los proveedores de servicios de comunicaciones electrónicas a comunicar mediante transmisión generalizada e indiferenciada datos de tráfico y de localización a las agencias de seguridad e inteligencia. En efecto, dicha transmisión tiene por efecto poner esos datos a disposición de las autoridades públicas [véase, por analogía, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 212].

80 Dado que la transmisión de los datos de tráfico y de localización tiene lugar de manera generalizada e indiferenciada, afecta de manera global a todas las personas que utilizan servicios de comunicaciones electrónicas. Por lo tanto, se aplica también a personas respecto de las cuales no existe ningún indicio que permita pensar que su comportamiento puede guardar relación, incluso indirecta o remota, con el objetivo de protección de la seguridad nacional y, en particular, sin que se acredite una relación entre los datos cuya transmisión se establece y una amenaza para la seguridad nacional (véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 57 y 58, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 105). Toda vez que la transmisión de tales datos a las autoridades públicas equivale, conforme a lo señalado en el apartado 79 de la presente sentencia, a un acceso, debe considerarse que una normativa que permite una transmisión generalizada e indiferenciada de los datos a las autoridades públicas implica un acceso general.

81 De ello resulta que una normativa nacional que obliga a los proveedores de servicios de comunicaciones electrónicas a comunicar a las agencias de seguridad e inteligencia mediante transmisión generalizada e indiferenciada datos de tráfico y de localización excede 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, interpretado a la luz del artículo 4 TUE, apartado 2, y de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta.

82 Habida cuenta de todas las consideraciones anteriores, procede responder a la segunda cuestión prejudicial que el artículo 15, apartado 1, de la Directiva 2002/58, a la luz del artículo 4 TUE, apartado 2, y de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una transmisión generalizada e indiferenciada de datos de tráfico y de localización a las agencias de seguridad e inteligencia con el fin de proteger la seguridad nacional.

Costas

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

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

1) **Los artículos 1, apartado 3, 3 y 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, a la luz del artículo 4 TUE, apartado 2, deben interpretarse en el sentido de que está comprendida en el ámbito de aplicación de esta Directiva una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a transmitir a las agencias de seguridad e inteligencia datos de tráfico y de localización con el fin de proteger la seguridad nacional.**

2) **El artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, a la luz del artículo 4 TUE, apartado 2, y de los artículos 7, 8 y 11 y del artículo 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 permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una transmisión generalizada e indiferenciada de datos de tráfico y de datos de localización a las agencias de seguridad e inteligencia con el fin de proteger la seguridad nacional.**

Firmas