Edición provisional

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 5 de abril de 2022 (*)

«Procedimiento prejudicial — Tratamiento de los datos personales en el sector de las comunicaciones electrónicas — Confidencialidad de las comunicaciones — Proveedores de servicios de comunicaciones electrónicas — Conservación generalizada e indiferenciada de los datos de tráfico y de localización — Acceso a los datos conservados — Control jurisdiccional a posteriori — Directiva 2002/58/CE — Artículo 15, apartado 1 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8, 11 y 52, apartado 1 — Posibilidad de que un órgano jurisdiccional nacional limite la eficacia temporal de una declaración de invalidez referida a una normativa nacional incompatible con el Derecho de la Unión — Exclusión»

En el asunto C-140/20,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Supreme Court (Tribunal Supremo, Irlanda), mediante resolución de 25 de marzo de 2020, recibida en el Tribunal de Justicia el mismo día, en el procedimiento entre

G. D.

y

Commissioner of An Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. K. Lenaerts, Presidente, el Sr. A. Arabadjiev, la Sra. A. Prechal y los Sres. S. Rodin, I. Jarukaitis y N. Jääskinen, Presidentes de Sala, y los Sres. T. von Danwitz (Ponente), M. Safjan, F. Biltgen, P. G. Xuereb y N. Piçarra, la Sra. L. S. Rossi y el Sr. A. Kumin, Jueces;

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

Secretario: Sr. D. Dittert, jefe de unidad;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 13 de septiembre de 2021;

consideradas las observaciones presentadas:

– en nombre de G. D., por el Sr. J. Dunphy, Solicitor, los Sres. R. Kennedy y R. Farrell, SC, y la Sra. K. McCormack, BL;

– en nombre del Commissioner of An Garda Síochána, el Minister for Communications, Energy and Natural Resources y el Attorney General, por las Sras. M. Browne, S. Purcell, C. Stone y J. Quaney y por el Sr. A. Joyce, en calidad de agentes, asistidos por los Sres. S. Guerin y P. Gallagher, SC, y por el Sr. D. Fennelly y la Sra. L. Dwyer, BL;

– 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;

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

– en nombre del Gobierno danés, inicialmente por los Sres. J. Nymann-Lindegren y M. Jespersen y por la Sra. M. Wolff, posteriormente por las Sras. M. Wolff y V. Jørgensen, en calidad de agentes;

– en nombre del Gobierno estonio, por las Sras. A. Kalbus y M. Kriisa, en calidad de agentes;

– en nombre del Gobierno español, por el Sr. L. Aguilera Ruiz, en calidad de agente;

– en nombre del Gobierno francés, por las Sras. E. de Moustier y A. Daniel y por los Sres. D. Dubois, T. Stéhelin y J. Illouz, en calidad de agentes;

– en nombre del Gobierno chipriota, por la Sra. I. Neophytou, en calidad de agente;

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

– en nombre del Gobierno polaco, por el Sr. B. Majczyna y la Sra. J. Sawicka, en calidad de agentes;

– en nombre del Gobierno portugués, por el Sr. L. Inez Fernandes y las Sras. P. Barros da Costa e I. Oliveira, en calidad de agentes;

– en nombre del Gobierno finlandés, por las Sras. M. Pere y A. Laine, en calidad de agentes;

– en nombre del Gobierno sueco, por los Sres. O. Simonsson y J. Lundberg y por las Sras. H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson y H. Eklinder, en calidad de agentes;

– en nombre de la Comisión Europea, por los Sres. S. L. Kalėda, H. Kranenborg, M. Wasmeier y F. Wilman, en calidad de agentes;

– en nombre del Supervisor Europeo de Protección de Datos, por los Sres. D. Nardi, N. Stolič y K. Ujazdowski y por la Sra. A. Buchta, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 18 de noviembre de 2021;

dicta la siguiente

Sentencia

1 La petición de decisión prejudicial tiene 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, 11 y 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 G. D. y el Commissioner of An Garda Síochána (jefe de la Policía nacional, Irlanda), el Minister for Communications, Energy and Natural Ressources (ministro de Comunicaciones, Energía y Recursos Naturales, Irlanda) y el Attorney General, en relación con la validez de la Communications (Retention of Data)

Act 2011 [Ley de 2011 sobre las Comunicaciones (Conservación de Datos); en lo sucesivo, «Ley de 2011»].

Marco jurídico

Derecho de la Unión

3 Los considerandos 2, 6, 7 y 11 de la Directiva 2002/58 exponen:

«(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 [aquella].

[…]

(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 [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.»

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 [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 [Tratado FUE], 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 A tenor del artículo 2 de la Directiva 2002/58, 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;

[…]».

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

7 A tenor del artículo 5 de esta Directiva, 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.»

8 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.

[…]»

9 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. […]»

10 El artículo 15 de la Directiva 2002/58, titulado «Aplicación de determinadas disposiciones de la Directiva [95/46]», dispone 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.»

Derecho irlandés

11 Como se deduce de la petición de decisión prejudicial, la Ley de 2011 se adoptó con el fin de transponer al ordenamiento jurídico irlandés 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).

12 El artículo 1 de la Ley de 2011 define el término «datos» como «los datos de tráfico y de localización y los datos conexos para identificar al abonado o usuario», y el término «delito grave» como un delito castigado con pena de prisión de una duración igual o superior a cinco años o uno de los demás delitos enumerados en el anexo 1 de esta Ley.

13 El artículo 3, apartado 1, de dicha Ley obliga a todos los proveedores de servicios de comunicaciones electrónicas a conservar los datos a que se refiere su anexo 2, parte 1, durante un período de dos años, así como los datos contemplados en su anexo 2, parte 2, durante un año.

14 El anexo 2, parte 1, de la misma Ley se refiere, entre otros, a los datos relativos a la telefonía fija y a la telefonía móvil que permiten identificar el origen y el destino de una comunicación, determinar la fecha y hora de inicio y fin de una comunicación, determinar el tipo de comunicación de que se trate e identificar el tipo y la localización geográfica del equipo de comunicación utilizado. En particular, el punto 6 de dicho anexo 2, parte 1, establece la conservación de los datos necesarios para localizar un medio de comunicación electrónica móvil, datos que son, por una parte, el identificador de celda y, por otra parte, los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización (el identificador de celda), durante el período en el que se conservan los datos de las comunicaciones.

15 El anexo 2, parte 2, de la Ley de 2011 se refiere a los datos relativos al acceso a Internet y al correo electrónico por Internet y telefonía por Internet, y comprende en particular los números de identificación y de teléfono, las direcciones IP, así como la fecha y hora de inicio y fin de una comunicación. El contenido de las comunicaciones no entra en esta categoría de datos.

16 En virtud de los artículos 4 y 5 de la Ley de 2011, los proveedores de servicios de comunicaciones electrónicas deben adoptar determinadas medidas para garantizar que los datos queden protegidos contra los accesos no autorizados.

17 El artículo 6 de esta Ley, que establece las condiciones en las que puede presentarse una solicitud de acceso, dispone en su apartado 1:

«Un funcionario de la Policía nacional de rango no inferior al de comisario de división podrá solicitar a un proveedor de servicios que le comunique los datos conservados por dicho proveedor de servicios de conformidad con el artículo 3 si el referido funcionario considera que los datos en cuestión son necesarios para:

(a) la prevención, el descubrimiento, la investigación o la persecución de delitos graves,

(b) la salvaguarda de la seguridad del Estado,

(c) la preservación de la vida humana.»

18 El artículo 7 de dicha Ley obliga a los proveedores de servicios de comunicaciones electrónicas a atender las solicitudes a que se refiere su artículo 6.

19 Entre los mecanismos de control de la resolución del funcionario de la Policía nacional mencionado en el artículo 6 de la Ley de 2011 figuran el procedimiento de reclamación previsto en el artículo 10 de dicha Ley y el procedimiento ante el *designated judge* (juez designado), en el sentido del artículo 12 de esta, que tiene por misión examinar la aplicación de las disposiciones de la citada Ley.

Litigio principal y cuestiones prejudiciales

20 En marzo de 2015, G. D. fue condenado a una pena de cadena perpetua por el asesinato de una persona que había desaparecido en agosto de 2012 y cuyos restos no se encontraron hasta septiembre de 2013. En la apelación de su condena, el interesado reprochó en particular al tribunal de primera instancia haber admitido erróneamente pruebas consistentes en datos de tráfico y de localización relativos a llamadas telefónicas, alegando que la Ley de 2011, que regulaba la conservación de esos datos y sirvió de fundamento legal a los investigadores de la Policía nacional para acceder a ellos, vulneraba los derechos que le confiere el Derecho de la Unión. Este recurso de apelación está aún por resolver.

21 Para poder impugnar en el proceso penal la admisibilidad de dichas pruebas, G. D. entabló ante la High Court (Tribunal Superior, Irlanda) un proceso civil dirigido a que se declarara la invalidez de determinadas disposiciones de la Ley de 2011. Mediante resolución de 6 de diciembre de 2018, este órgano jurisdiccional estimó las alegaciones de G. D. y consideró que el artículo 6, apartado 1, letra a), de dicha Ley era incompatible con el artículo 15, apartado 1, de la Directiva 2002/58 a la vista de los artículos 7, 8 y 52, apartado 1, de la Carta. Irlanda ha interpuesto recurso de apelación contra esta resolución ante la Supreme Court (Tribunal Supremo, Irlanda), el órgano jurisdiccional remitente.

22 El proceso penal que pende ante la Court of Appeal (Tribunal de Apelación, Irlanda) se suspendió hasta que se dicte la resolución del órgano jurisdiccional remitente en el marco del proceso civil principal.

23 Ante el órgano jurisdiccional remitente, Irlanda sostuvo que, para determinar si la injerencia en el derecho al respeto de la vida privada consagrado en el artículo 7 de la Carta que implica la conservación de los datos de tráfico y de localización en virtud de la Ley de 2011 es proporcionada, deben examinarse de manera conjunta los objetivos del régimen instaurado por esta Ley. Además, según el citado Estado miembro,

dicha Ley estableció un marco detallado que regula el acceso a los datos conservados, en virtud del cual la unidad encargada del examen previo de las solicitudes de acceso ejerce sus funciones con plena independencia dentro de la Policía nacional en la que se halla integrada y, por consiguiente, satisface el requisito del control previo efectuado por un organismo administrativo independiente, existiendo además un procedimiento de reclamación y un control jurisdiccional que completan ese control. Finalmente, dicho Estado miembro alega que, si se considera, en definitiva, que la Ley de 2011 es contraria al Derecho de la Unión, cualquier conclusión a la que llegue el órgano jurisdiccional remitente sobre esa base debería desplegar sus efectos exclusivamente hacia el futuro.

24 Por su parte, G. D. alegó que el régimen de conservación generalizada e indiferenciada de los datos y el régimen de acceso a estos que ha establecido la Ley de 2011 son incompatibles con el Derecho de la Unión tal como lo ha interpretado, en particular, el Tribunal de Justicia en el apartado 120 de la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970).

25 El órgano jurisdiccional remitente indica, con carácter preliminar, que solo le corresponde apreciar si la High Court (Tribunal Superior) declaró acertadamente que el artículo 6, apartado 1, letra a), de la Ley de 2011 es incompatible con el Derecho de la Unión y que, en cambio, pronunciarse sobre la admisibilidad de las pruebas propuestas en el proceso penal es competencia exclusiva de la Court of Appeal (Tribunal de Apelación), que conoce del recurso interpuesto contra la resolución condenatoria.

26 En este contexto, el órgano jurisdiccional remitente alberga dudas, en primer término, sobre las exigencias del Derecho de la Unión en materia de conservación de datos con fines de lucha contra la delincuencia grave. A este respecto, estima, en esencia, que solo una conservación generalizada e indiferenciada de los datos de tráfico y de localización permite luchar eficazmente contra la delincuencia grave y que, en cambio, una conservación selectiva y una conservación rápida (*quick freeze*) no resultarían tan eficaces. Por lo que respecta a la conservación selectiva, el órgano jurisdiccional remitente alberga dudas sobre la posibilidad de centrarse en grupos o zonas geográficas determinados a efectos de la lucha contra la delincuencia grave, en la medida en que ciertos delitos graves rara vez implican circunstancias que las autoridades nacionales competentes conozcan y que permitan a estas sospechar con anticipación la comisión de un delito, además de que una conservación selectiva puede dar lugar a discriminaciones. En cuanto a la conservación rápida, el órgano jurisdiccional remitente considera que solo es

útil en situaciones en las que existe un sospechoso que puede ser identificado en una fase temprana de la investigación.

27 A continuación, en lo tocante al acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas, el órgano jurisdiccional remitente recalca que en el seno de la Policía nacional se instauró un mecanismo de autocertificación de las solicitudes de acceso dirigidas a esos proveedores. De esta manera, las pruebas aportadas ante la High Court (Tribunal Superior) ponen de manifiesto que el jefe de la Policía nacional decidió, como medida interna, que las solicitudes de acceso presentadas con arreglo a la Ley de 2011 deben ser tratadas de forma centralizada por un único agente de la Policía nacional, en calidad de comisario de división, es decir, el jefe de la Sección de Seguridad e Inteligencia. Si este último considera que los datos de que se trata son necesarios, en particular, para la prevención, el descubrimiento, la investigación o la persecución de un delito grave, podrá dirigir una solicitud de acceso a los proveedores de servicios de comunicaciones electrónicas. El órgano jurisdiccional remitente explica que, por otra parte, el jefe de la Policía nacional creó una unidad autónoma, aunque integrada en esta, denominada «Telecommunications Liaison Unit» (Unidad de Enlace en Materia de Telecomunicaciones; en lo sucesivo, «TLU»), con el fin de prestar apoyo al jefe de la Sección de Seguridad e Inteligencia en el ejercicio de sus funciones y actuar como único punto de contacto con esos mismos proveedores de servicios.

28 El órgano jurisdiccional remitente añade que, durante el período abarcado por la investigación penal iniciada contra G. D., todas las solicitudes de acceso debían ser aprobadas en primer lugar por un comisario o un inspector en funciones de comisario, antes de ser enviadas a la TLU para su tramitación, y que se invitaba a los investigadores a que cumplimentaran sus solicitudes de acceso de manera suficientemente detallada para que pudiera adoptarse una decisión bien informada. Además, la TLU y el jefe de la Sección de Seguridad e Inteligencia estaban obligados a examinar la legalidad, la necesidad y la proporcionalidad de las solicitudes de acceso, teniendo en cuenta que dicho jefe podía ser requerido para que justificara su decisión ante un juez designado por la High Court (Tribunal Superior). El órgano jurisdiccional remitente indica, por otra parte, que la TLU está sujeta al control del Data Protection Commissioner (comisario para la protección de datos, Irlanda).

29 Por último, el órgano jurisdiccional remitente alberga dudas sobre el alcance y los efectos en el tiempo de una eventual declaración de incompatibilidad de

la Ley de 2011 con el Derecho de la Unión. A este respecto, indica que tal declaración solo podría ser válida para el futuro, ya que los datos utilizados como prueba en el proceso penal contra G. D. fueron conservados y se accedió a ellos a finales de 2013, a saber, en un tiempo en el que Irlanda estaba obligada a aplicar las disposiciones de la Ley de 2011 por las que se transponía la Directiva 2006/24. Según Irlanda, tal solución sería tanto más adecuada cuanto que, en caso contrario, podrían resultar seriamente afectadas tanto la investigación y la persecución de los delitos graves en Irlanda como la situación de personas ya juzgadas y condenadas.

30 En tales circunstancias, la Supreme Court (Tribunal Supremo) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Un régimen general o universal de conservación de datos, aunque esté sujeto a restricciones rigurosas tanto por lo que se refiere a la conservación como al acceso de los datos, es *per se* contrario a las disposiciones del artículo 15 de la Directiva [2002/58], interpretado a la luz de la Carta?

2) A la hora de decidir si es contraria al Derecho de la Unión una medida nacional, aplicada sobre la base de la Directiva [2006/24], que establece un régimen general de conservación de datos sujeto a los necesarios controles estrictos en materia de conservación y de acceso a los mismos, y, en particular, a la hora de valorar la proporcionalidad de dicho régimen, ¿es lícito que un órgano jurisdiccional nacional tenga en cuenta el hecho de que los proveedores del servicio pueden legalmente conservar los datos para sus propios fines comerciales y se les puede exigir que conserven esos datos por razones de seguridad nacional excluidas de las disposiciones de la Directiva [2002/58]?

3) ¿Qué criterios debería aplicar un órgano jurisdiccional nacional, en el examen de la compatibilidad con el Derecho de la Unión Europea y, en particular, con la Carta, de una medida nacional relativa al acceso a los datos conservados, para determinar si tal régimen de acceso contempla el control previo independiente exigido según la jurisprudencia del Tribunal de Justicia? En dicho contexto ¿puede un órgano jurisdiccional nacional, al hacer tal valoración, tener en cuenta la existencia de un control judicial o independiente posterior?

4) En cualquier caso, ¿está un órgano jurisdiccional nacional obligado a declarar una medida nacional contraria a las disposiciones del artículo

15 de la Directiva [2002/58] si dicha medida establece un régimen general de conservación de datos a los fines de la lucha contra los delitos graves y el órgano jurisdiccional nacional ha llegado a la conclusión, de acuerdo con todas las pruebas disponibles, de que tal conservación de datos es esencial y estrictamente necesaria para alcanzar los fines de la lucha contra los delitos graves?

5) ¿Si un órgano jurisdiccional nacional está obligado a concluir que una medida nacional es contraria a las disposiciones del artículo 15 de la Directiva [2002/58], interpretado a la luz de la Carta, puede lícitamente limitar el efecto temporal de dicha declaración si entiende que, de no hacerlo, se causaría un "desorden y perjuicio para el interés general" [en línea, por ejemplo, con el enfoque adoptado en el asunto R (National Council for Civil Liberties) contra Secretary of State for Home Department y Secretary of State for Foreign Affairs [2018] EWHC 975, apartado 46]?

6) ¿Está autorizado un órgano jurisdiccional nacional al que se le pide que declare que la legislación nacional es contraria al artículo 15 de la Directiva [2002/58] o que no aplique dicha legislación o que declare que su aplicación ha vulnerado los derechos de una persona, en el contexto de un procedimiento iniciado para defender una posición respecto de la admisibilidad de las pruebas en un proceso penal o en cualquier otra circunstancia, a denegar tal pretensión en lo que se refiere a los datos conservados con arreglo a una disposición nacional aprobada en virtud de la obligación, impuesta por el artículo 288 TFUE, de incorporar fielmente a la legislación nacional las disposiciones de una directiva, o a limitar tal declaración al período posterior a la sentencia [de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238),] por la que se declara la invalidez de la Directiva [2006/24]?»

Sobre las cuestiones prejudiciales

Cuestiones prejudiciales primera, segunda y cuarta

31 Mediante sus cuestiones prejudiciales primera, segunda y cuarta, que deben examinarse conjuntamente, el órgano jurisdiccional remitente desea que se dilucide, en esencia, si 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 una conservación generalizada e indiferenciada de los datos de tráfico y de localización con fines de lucha contra la delincuencia grave.

32 Conviene recordar, con carácter preliminar, que, según reiterada jurisprudencia, para la interpretación de una disposición del Derecho de la Unión, no solo hay que referirse al tenor de esta, sino también tener en cuenta su contexto y los objetivos perseguidos por la normativa de la que forma parte, así como tomar en consideración, en especial, la génesis de esa normativa (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 105 y jurisprudencia citada).

33 Del propio tenor del artículo 15, apartado 1, de la Directiva 2002/58 se desprende que las medidas legales que esta autoriza a los Estados miembros a adoptar, en las condiciones que en ella se establecen, únicamente pueden ir dirigidas a «limitar el alcance» de los derechos y las obligaciones establecidos en particular en los artículos 5, 6 y 9 de la Directiva 2002/58.

34 En cuanto al sistema instaurado por la citada Directiva y en el que se inserta su artículo 15, apartado 1, procede recordar que, en virtud del artículo 5, apartado 1, frases primera y segunda, de dicha Directiva, los Estados miembros están obligados a garantizar, mediante su legislación nacional, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público, así como la confidencialidad de los datos de tráfico asociados a ellas. En particular, están obligados a prohibir 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 artículo 15, apartado 1, de la misma Directiva.

35 A este respecto, el Tribunal de Justicia ya ha declarado que el artículo 5, apartado 1, de la Directiva 2002/58 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 (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 107).

36 La citada disposición refleja el objetivo perseguido por el legislador de la Unión al adoptar la Directiva 2002/58. En efecto, 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». De esta manera, la citada Directiva tiene por finalidad, como se infiere 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, como se dice en el considerando 2 de la misma Directiva, la voluntad del legislador de la Unión es garantizar el pleno respeto de los derechos reconocidos en los artículos 7 y 8 de la Carta (véanse, en este sentido, las sentencias de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartado 83, 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 106).

37 A través de la adopción de la Directiva 2002/58, el legislador de la Unión concretó esos derechos, de suerte 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).

38 Por lo que se refiere al tratamiento y almacenamiento por parte de los proveedores de servicios de comunicaciones electrónicas de los datos de tráfico relativos a abonados y usuarios, el artículo 6 de la Directiva 2002/58 establece, en su apartado 1, que esos datos deberán eliminarse o hacerse anónimos cuando ya no sean necesarios para la transmisión de una comunicación e indica, en su apartado 2, que podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones solamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. En cuanto a los datos de localización distintos de los datos de tráfico, el artículo 9, apartado 1, de dicha Directiva establece que esos datos solo podrán tratarse en ciertas

condiciones, si se hacen anónimos, o previo consentimiento de los usuarios o abonados.

39 Por lo tanto, la Directiva 2002/58 no se limita a regular el acceso a tales datos mediante garantías dirigidas a prevenir los abusos, sino que también consagra, en particular, el principio de prohibición de su almacenamiento por terceros.

40 En la medida en que el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros adoptar medidas legales para «limitar el alcance» de los derechos y obligaciones que se establecen en particular en los artículos 5, 6 y 9 de esta Directiva, como los derivados de los principios de confidencialidad de las comunicaciones y de prohibición de almacenamiento de los datos asociados a ellas, recordados en el apartado 35 de la presente sentencia, tal disposición introduce una excepción a la regla general establecida, en particular, en dichos artículos 5, 6 y 9, por lo que, conforme a reiterada jurisprudencia, debe ser objeto de una interpretación estricta. En consecuencia, tal disposición 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, prevista en el artículo 5 de la citada Directiva, se convierta en la regla si no se quiere privar en gran medida a esta última disposición de su alcance (véanse, en este sentido, las sentencias de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartado 89, 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).

41 Por lo que respecta a los objetivos que pueden justificar una limitación de los derechos y de las obligaciones previstos, en particular, en los artículos 5, 6 y 9 de la Directiva 2002/58, el Tribunal de Justicia ya ha declarado que la enumeración de los objetivos que figuran en el artículo 15, apartado 1, primera frase, de dicha Directiva tiene carácter exhaustivo, de modo que la medida legal que se adopte en virtud de esta disposición ha de responder efectiva y estrictamente a uno de ellos (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 112 y jurisprudencia citada).

42 Además, del artículo 15, apartado 1, tercera frase, de la Directiva 2002/58 se infiere que las medidas adoptadas por los Estados miembros con arreglo a esta disposición deben respetar los principios generales del Derecho de la Unión, entre los que figura el principio de proporcionalidad, y 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 dudas 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 datos de carácter personal, respectivamente, sino también del artículo 11 de la Carta, relativo a la libertad de expresión (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 113 y jurisprudencia citada).

43 De esta manera, 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 garantizado por el artículo 8 de esta, tal como se desprende de la jurisprudencia del Tribunal de Justicia, como del derecho a la libertad de expresión, que es un derecho fundamental, garantizado por 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 (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 114 y jurisprudencia citada).

44 Debe precisarse a este respecto que la conservación de los datos de tráfico y de localización constituye, por sí sola, por una parte, una excepción a la prohibición, establecida en el artículo 5, apartado 1, de la Directiva 2002/58, de que cualquier persona distinta de los usuarios almacene dichos datos y, por otra parte, una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal, consagrados en los artículos 7 y 8 de la Carta, siendo irrelevante 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 (véase, en este sentido, 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 y jurisprudencia citada).

45 Esta conclusión parece tanto más justificada cuanto que los datos de tráfico y de localización pueden revelar información sobre un número considerable de aspectos de la vida privada de las personas de que se trate, incluida información de carácter sensible, como la orientación sexual, las opiniones políticas, las creencias religiosas, filosóficas, sociales u otras y el estado de salud, dado que estos datos gozan, además, de una protección particular en el

Derecho de la Unión. Considerados en su conjunto, estos datos pueden permitir 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. En particular, estos datos proporcionan medios para determinar 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 (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 117 y jurisprudencia citada).

46 En consecuencia, por una parte, la conservación de datos de tráfico y de localización con fines policiales puede vulnerar el derecho al respeto de las comunicaciones, consagrado en el artículo 7 de la Carta, y disuadir a los usuarios de los medios de comunicaciones electrónicas de ejercer su libertad de expresión, garantizada por el artículo 11 de la Carta, efectos que son especialmente graves, dada la cantidad y la variedad de datos conservados. Por otra parte, 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 e indiferenciada 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 (véase, en este sentido, 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 118 y 119 y jurisprudencia citada).

47 A este respecto, se ha de destacar que la conservación de esos datos y el acceso a ellos constituyen, como se desprende de la jurisprudencia recordada en el apartado 44 de la presente sentencia, injerencias distintas en los derechos fundamentales garantizados por los artículos 7 y 11 de la Carta que requieren una justificación distinta, con arreglo al artículo 52, apartado 1, de esta. Por lo tanto, una normativa nacional que cumpla estrictamente los requisitos formulados por la jurisprudencia relativa a la Directiva 2002/58 en materia de acceso a los datos conservados no puede, por naturaleza, ni limitar ni menos aún subsanar la injerencia grave, originada por la conservación generalizada de tales datos con arreglo a esa normativa nacional, en los derechos garantizados por los artículos 5 y 6 de dicha Directiva y por los derechos fundamentales que quedaron determinados mediante estos artículos.

48 Ahora bien, en la medida en que permite a los Estados miembros limitar los derechos y las obligaciones mencionados en los apartados 34 a 37 de la presente sentencia, el artículo 15, apartado 1, de la Directiva 2002/58 refleja el hecho de que los derechos consagrados en los artículos 7, 8 y 11 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse de acuerdo con su función en la sociedad. En efecto, como se desprende del artículo 52, apartado 1, de la Carta, esta admite limitaciones al ejercicio de esos derechos, siempre que se establezcan por ley, respeten el contenido esencial de los citados derechos y, ajustándose al 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. De este modo, la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 a la luz de la Carta exige tener en cuenta asimismo la importancia de los derechos consagrados en los artículos 3, 4, 6 y 7 de la Carta y la que presentan los objetivos de protección de la seguridad nacional y de lucha contra la delincuencia grave al contribuir a la protección de los derechos y de las libertades de terceros (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 120 a 122 y jurisprudencia citada).

49 De esta manera, por lo que respecta, específicamente, a la lucha efectiva contra los delitos perpetrados, en particular, contra los menores y otras personas vulnerables, debe tenerse en cuenta que del artículo 7 de la Carta pueden resultar obligaciones positivas que incumban a los poderes públicos, con miras a la adopción de medidas jurídicas dirigidas a proteger la vida privada y familiar. Estas obligaciones pueden resultar asimismo de dicho artículo 7 por lo que se refiere a la protección del domicilio y de las comunicaciones, así como de los artículos 3 y 4 en lo tocante a la protección de la integridad física y psíquica de la persona y a la prohibición de la tortura y de los tratos inhumanos o degradantes (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 126 y jurisprudencia citada).

50 En consecuencia, frente a estas diferentes obligaciones positivas, conviene proceder a una conciliación necesaria de los distintos intereses y derechos en juego. En efecto, el Tribunal Europeo de Derechos Humanos ha declarado que las obligaciones positivas resultantes de los artículos 3 y 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, cuyas garantías correspondientes figuran en los artículos 4 y 7 de la Carta, implican, en particular, la adopción de disposiciones materiales y procesales, así como de medidas prácticas que permitan combatir eficazmente los delitos contra las personas mediante una investigación y un

enjuiciamiento efectivos, siendo esta obligación aún más importante cuando existe una amenaza para el bienestar físico y moral de un niño. Dicho esto, las medidas que incumbe adoptar a las autoridades competentes deben respetar plenamente las vías legales y las demás garantías susceptibles de limitar el alcance de las facultades de investigación penal, así como los demás derechos y libertades. En particular, según este órgano jurisdiccional, es preciso establecer un marco jurídico que permita conciliar los distintos intereses legítimos y derechos que se han de proteger (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 127 y 128 y jurisprudencia citada).

51 En este marco, de los propios términos del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 se infiere que los Estados miembros podrán adoptar una medida que suponga una excepción al principio de confidencialidad al que se ha hecho referencia en el apartado 35 de la presente sentencia, cuando tal medida sea «necesaria, proporcionada y apropiada en una sociedad democrática», mientras que el considerando 11 de esta Directiva precisa que una medida de esta naturaleza debe ser «rigurosamente» proporcionada al objetivo que pretende lograr (véase, en este sentido, 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, apartado 129).

52 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, efectuando una ponderación equilibrada entre, por una parte, el objetivo de interés general y, por otra parte, los intereses y derechos de que se trate (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 130 y jurisprudencia citada).

53 Más concretamente, de la jurisprudencia del Tribunal de Justicia se desprende que la posibilidad de que los Estados miembros justifiquen una limitación de los derechos y obligaciones previstos, en particular, en los artículos 5, 6 y 9 de la Directiva 2002/58 debe apreciarse determinando la gravedad de la injerencia que supone esa limitación y comprobando que la importancia del objetivo de interés general perseguido por dicha limitación guarde relación con tal gravedad (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 131 y jurisprudencia citada).

54 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 contra 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 especialmente aplicables cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles (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 132 y jurisprudencia citada).

55 De este modo, una normativa nacional que establezca la conservación de los datos de carácter personal debe responder en todo caso a criterios objetivos y ha de existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr. En particular, en lo que respecta a la lucha contra la delincuencia grave, los datos que van a ser conservados deben ser tales que contribuyan a la prevención, detección o enjuiciamiento de delitos graves (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 59, 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 133).

56 Por lo que toca a los objetivos de interés general que permiten justificar una medida adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58, de la jurisprudencia del Tribunal de Justicia, en particular de 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), se desprende que, conforme al principio de proporcionalidad, existe una jerarquía entre dichos objetivos en función de su importancia respectiva y que la importancia del objetivo perseguido por tal medida debe ser correlativa a la gravedad de la injerencia que supone la medida.

57 A este respecto, el Tribunal de Justicia ha declarado que la importancia del objetivo de protección de la seguridad nacional, interpretado a la luz del artículo 4 TUE, apartado 2, según el cual la protección de la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro, supera la de los demás objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, en particular los objetivos de combatir la delincuencia en general, incluso grave, y de protección de 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 (véase, en este sentido, 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 135 y 136).

58 Esta es la razón por la que el Tribunal de Justicia ha declarado 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, no se opone a medidas legislativas que permitan, a efectos de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en situaciones en las que el Estado miembro en cuestión se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, pudiendo ser objeto la decisión que contenga dicho requerimiento de un control efectivo bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, que tenga por objeto comprobar la existencia de una de estas situaciones, así como el respecto de las condiciones y de las garantías que deben establecerse, y teniendo en cuenta que dicho requerimiento únicamente podrá expedirse por un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse en caso de que persista dicha amenaza (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 168).

59 En lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos, el Tribunal de Justicia ha señalado que, de conformidad con el principio de proporcionalidad, solo la lucha contra la delincuentica grave y la prevención de las amenazas graves contra la seguridad pública pueden justificar las injerencias graves en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, como las que supone la conservación de los datos de tráfico y de los datos de localización.

En consecuencia, solo las injerencias en tales derechos fundamentales que no presenten un carácter grave pueden estar justificadas por el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general (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 140 y jurisprudencia citada).

60 En la vista, la Comisión Europea sostuvo que la delincuencia especialmente grave podría asimilarse a una amenaza para la seguridad nacional.

61 Pues bien, el Tribunal de Justicia ya ha declarado que el objetivo de protección de la seguridad nacional 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, y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado, tales como las actividades terroristas (véase, en este sentido, 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, apartado 135).

62 Es pertinente señalar asimismo que, a diferencia de la delincuencia, aunque sea especialmente grave, una amenaza para la seguridad nacional debe ser real y actual, o cuando menos previsible, lo que supone que surjan circunstancias suficientemente concretas para poder justificar una medida de conservación generalizada e indiferenciada de datos de tráfico y de localización, durante un plazo limitado. Así pues, tal amenaza se distingue, por su naturaleza, su gravedad y el carácter específico de las circunstancias que la forman y del riesgo general y permanente de que surjan tensiones o perturbaciones, incluso graves, que afecten a la seguridad pública o del riesgo de delitos graves (véase, en este sentido, 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 136 y 137).

63 La delincuencia, aunque sea especialmente grave, no puede asimilarse, pues, a una amenaza para la seguridad nacional. En efecto, como señaló el Abogado General en los puntos 49 y 50 de sus conclusiones, tal asimilación podría implicar la introducción de una categoría intermedia entre la seguridad nacional y la seguridad pública para aplicar a la segunda las exigencias inherentes a la primera.

64 De ello se sigue igualmente que la circunstancia, mencionada en la segunda cuestión prejudicial, de que los datos de tráfico y los datos de localización hayan sido legalmente objeto de conservación a efectos de la protección de la seguridad nacional no afecta a la licitud de su conservación con fines de lucha contra la delincuencia grave.

65 Por lo que respecta al objetivo de lucha contra la delincuencia grave, el Tribunal de Justicia ha declarado que una normativa nacional que establece, a tales efectos, la conservación generalizada e indiferenciada de los datos de tráfico y de localización excede de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática. En efecto, habida cuenta del carácter sensible de la información que pueden proporcionar los datos de tráfico y de localización, la confidencialidad de estos es fundamental para el derecho al respeto de la vida privada. De este modo, y teniendo en cuenta, por una parte, los efectos disuasorios sobre el ejercicio de los derechos fundamentales consagrados en los artículos 7 y 11 de la Carta, a los que se ha hecho referencia en el apartado 46 de la presente sentencia, que la conservación de estos datos puede acarrear y, por otra parte, la gravedad de la injerencia que supone dicha conservación, es importante que en una sociedad democrática tal conservación constituya, como prevé el sistema establecido por la Directiva 2002/58, la excepción y no la regla y que esos datos no puedan ser objeto de una conservación sistemática y continua. Esta conclusión se impone incluso respecto de los objetivos de lucha contra la delincuencia grave y de prevención de las amenazas graves contra la seguridad pública, así como de la importancia que se les debe reconocer (véase, en este sentido, 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 141 y 142 y jurisprudencia citada).

66 Por otro lado, el Tribunal de Justicia ha recalcado que una normativa que prevé la conservación generalizada e indiferenciada de los datos de tráfico y de localización abarca las comunicaciones electrónicas de prácticamente toda la población sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo perseguido. Tal normativa afecta con carácter global a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que estas personas se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales. Por lo tanto, se aplica incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remotamente, con dicho objetivo de lucha contra la delincuencia grave y, en particular, sin que se establezca una relación entre los datos cuya conservación se prevé y una amenaza para la seguridad pública. En particular, como ya ha declarado

el Tribunal de Justicia, tal normativa 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 grave (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 143 y 144 y jurisprudencia citada).

67 En cambio, en el apartado 168 de 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), el Tribunal de Justicia señaló 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, no se opone a medidas legislativas que establezcan, a efectos de la lucha contra la delincuencia grave y de la prevención de amenazas graves contra la seguridad pública,

– una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse;

– una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;

– una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y

– el recurso a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida (*quick freeze*) de los datos de tráfico y de localización de que dispongan estos proveedores de servicios,

siempre que dichas medidas garanticen, mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso.

68 En la presente petición de decisión prejudicial, que se recibió en el Tribunal de Justicia antes de que se pronunciaran las sentencias 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), y de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, EU:C:2021:152), el órgano jurisdiccional remitente ha considerado no obstante que solo una conservación generalizada e indiferenciada de los datos de tráfico y de localización permitiría luchar eficazmente contra la delincuencia grave. En la vista de 13 de septiembre de 2021, Irlanda y el Gobierno francés sostuvieron que tal conclusión no quedaba desvirtuada por el hecho de que los Estados miembros puedan recurrir a las medidas mencionadas en el apartado anterior.

69 A este respecto, se ha de señalar, en primer lugar, que la eficacia de las acciones penales depende generalmente no de un solo medio de investigación, sino de todos los medios de investigación que se hallen a disposición de las autoridades nacionales competentes a los referidos efectos.

70 En segundo lugar, procede recalcar 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, tal como ha sido interpretado por la jurisprudencia recordada en el apartado 67 de la presente sentencia, permite a los Estados miembros adoptar, a efectos de la lucha contra la delincuencia grave y de la prevención de amenazas graves contra la seguridad pública, no solo medidas que establezcan una conservación selectiva y una conservación rápida, sino también medidas dirigidas a una conservación generalizada e indiferenciada, por un lado, de los datos relativos a la identidad civil de los usuarios de medios de comunicación electrónica y, por otro, de las direcciones IP atribuidas al origen de una conexión.

71 A este respecto, consta que la conservación de los datos relativos a la identidad civil de los usuarios de los medios de comunicación electrónica puede contribuir a la lucha contra la delincuencia grave, siempre que esos datos permitan identificar a las personas que han utilizado tales medios en el contexto de la preparación o la comisión de un acto delictivo grave.

72 Pues bien, como se desprende de la jurisprudencia resumida en el apartado 67 de la presente sentencia, la Directiva 2002/58 no se opone, a efectos de la lucha contra la delincuencia en general, a la conservación generalizada de los datos relativos a la identidad civil. En tal contexto, debe observarse que ni esta Directiva ni ningún otro acto del Derecho de la Unión se oponen a una normativa nacional, que tenga por objeto la lucha contra la delincuencia

grave, en virtud de la cual la adquisición de un medio de comunicación electrónica, como una tarjeta SIM de prepago, está supeditada a la comprobación de documentos oficiales que acrediten la identidad del comprador y al registro, por el vendedor, de la información obtenida por tal vía, estando el vendedor, en su caso, obligado a permitir a las autoridades nacionales competentes que accedan a esa información.

73 Además, procede recordar que la conservación generalizada de las direcciones IP del origen de la conexión constituye una injerencia grave en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, toda vez que tales direcciones IP pueden permitir extraer conclusiones precisas sobre la vida privada del usuario del medio de comunicación electrónica de que se trate y puede tener efectos disuasorios sobre el ejercicio de la libertad de expresión garantizada en el artículo 11 de la Carta. No obstante, respecto de tal conservación, el Tribunal de Justicia ha señalado que debe tenerse en cuenta, a efectos de la necesaria conciliación de los derechos y de los intereses legítimos en cuestión exigida por la jurisprudencia a la que se ha hecho referencia en los apartados 50 a 53 de la presente sentencia, el hecho de que, en caso de un delito cometido en línea y, en particular, en caso de la adquisición, la difusión, la transmisión o la puesta a disposición en línea de pornografía infantil, en el sentido del artículo 2, letra c), de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión Marco 2004/68/JAI del Consejo (DO 2011, L 335, p. 1), la dirección IP puede constituir el único método de investigación para identificar a la persona a la que se atribuyó esa dirección en el momento en que se cometió dicho delito (véase, en este sentido, 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 153 y 154).

74 Por lo tanto, el Tribunal de Justicia ha declarado que tal conservación generalizada e indiferenciada únicamente de las direcciones IP atribuidas al origen de una conexión no resulta, en principio, contraria al artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 de la Carta, siempre que esta posibilidad esté sujeta al estricto cumplimiento de los requisitos materiales y procedimentales que deben regir la utilización de esos datos a los que se hizo referencia en los apartados 155 y 156 de 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).

75 En tercer lugar, por lo que toca a las medidas legislativas que establecen una conservación selectiva y una conservación rápida de los datos de tráfico y de localización, en la petición de decisión prejudicial se les atribuye un alcance más limitado que el propugnado por la jurisprudencia citada en el apartado 67 de la presente sentencia. En efecto, si bien, conforme a lo que se ha recordado en el apartado 40 de la presente sentencia, esas medidas de conservación deben constituir una excepción dentro del sistema instaurado por la Directiva 2002/58, esta última, interpretada a la luz de los derechos fundamentales consagrados en los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no sujeta la posibilidad de expedir un requerimiento que imponga una conservación selectiva al requisito de que se conozcan de antemano los lugares que pueden ser escenario de un acto delictivo grave ni las personas sospechosas de estar implicadas en tal acto. De igual forma, dicha Directiva no exige que el requerimiento que impone una conservación rápida se limite a los sospechosos que ya habían sido antes identificados.

76 Para empezar, por lo que se refiere a la conservación selectiva, el Tribunal de Justicia ha declarado que el artículo 15, apartado 1, de la Directiva 2002/58 no se opone a una normativa nacional basada en elementos objetivos, que permitan dirigirse, por un lado, a las personas cuyos datos de tráfico y de localización puedan presentar una relación, por lo menos indirecta, con delitos graves, contribuir a la lucha contra la delincuencia grave o prevenir un riesgo grave para la seguridad pública o incluso un riesgo para la seguridad nacional (sentencias de 21 de diciembre de 2016, Tele2 Sverige et Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartado 111, así como 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 148).

77 El Tribunal de Justicia ha señalado al respecto que, si bien tales elementos objetivos pueden variar en función de las medidas adoptadas a efectos de la prevención, la investigación, el descubrimiento y la persecución de la delincuencia grave, dichas personas pueden, en particular, ser aquellas que han sido identificadas previamente, en el marco de procedimientos nacionales aplicables y sobre la base de elementos objetivos y no discriminatorios, como una amenaza para la seguridad pública o la seguridad nacional del Estado miembro en cuestión (véanse, en este sentido, las sentencias de 21 de diciembre de 2016, Tele2 Sverige et Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartado 110, 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 149).

78 De esta manera, los Estados miembros tienen la facultad de adoptar medidas de conservación sobre personas a las que se identifica porque están siendo

investigadas o están siendo objeto de otras medidas de vigilancia o constan en el registro nacional de antecedentes penales por una condena anterior por delitos graves que pueden implicar un elevado riesgo de reincidencia. Pues bien, si tal identificación se basa en elementos objetivos y no discriminatorios, definidos por el Derecho nacional, la conservación selectiva concerniente a personas identificadas de este modo está justificada.

79 Por otro lado, una medida de conservación selectiva de datos de tráfico y de localización puede fundarse asimismo, según la elección del legislador nacional y respetándose estrictamente el principio de proporcionalidad, en un criterio geográfico si las autoridades nacionales competentes consideran, sobre la base de elementos objetivos y no discriminatorios, que existe una situación caracterizada por un riesgo elevado de preparación o de comisión de delitos graves en una o varias zonas geográficas. Estas zonas pueden ser, en particular, lugares en los que se produce un número elevado de delitos graves, lugares especialmente expuestos a la comisión de delitos graves, como los lugares o infraestructuras a los que acuden con regularidad un número muy elevado de personas, o incluso lugares estratégicos, como aeropuertos, estaciones de ferrocarril, puertos marítimos o zonas de peajes (véase, en este sentido, 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, apartado 150 y jurisprudencia citada).

80 Conviene destacar que, según esta jurisprudencia, las autoridades nacionales competentes pueden adoptar, para las zonas mencionadas en el apartado anterior, una medida de conservación selectiva fundada en un criterio geográfico, como, en particular, la tasa media de delincuencia en una zona geográfica, sin que dispongan necesariamente de indicios concretos sobre la preparación o la comisión de delitos graves en las zonas de que se trata. En la medida en que una conservación selectiva fundada en tal criterio puede afectar, en función de los delitos graves contemplados y de la situación específica de los Estados miembros respectivos, tanto a lugares en los que se produce un elevado número de delitos graves como a los lugares especialmente expuestos a la comisión de tales delitos, en principio, tampoco puede dar lugar a discriminaciones, pues el criterio relativo a la tasa media de delincuencia grave no presenta, en sí mismo, ningún vínculo con elementos potencialmente discriminatorios.

81 Al fin y al cabo, una medida de conservación selectiva referida a lugares o infraestructuras frecuentadas regularmente por un número muy elevado de personas o lugares estratégicos, como aeropuertos, estaciones de ferrocarril, puertos marítimos o zonas de peajes, permite a las autoridades competentes

obtener datos de tráfico y, en particular, datos de localización de todas las personas que utilizan en un momento dado un medio de comunicación electrónica en uno de esos lugares. De esta manera, tal medida de conservación selectiva puede permitir a dichas autoridades obtener, mediante el acceso a los datos así conservados, información sobre la presencia de esas personas en los lugares o zonas geográficas objeto de la expresada medida, así como sobre sus desplazamientos entre o dentro de tales lugares o zonas y extraer conclusiones, a efectos de la lucha contra la delincuencia grave, sobre su presencia y su actividad en esos lugares o zonas geográficas en un momento dado durante el período de conservación.

82 Debe señalarse asimismo que las zonas geográficas a las que se refiere tal conservación selectiva pueden y, en su caso, deben modificarse en función de la evolución de las condiciones que justificaron su selección, permitiendo así, en particular, reaccionar al compás de los progresos en la lucha contra la delincuencia grave. En efecto, el Tribunal de Justicia ya ha declarado que la duración de las medidas de conservación selectiva descritas en los apartados 76 a 81 de la presente sentencia no debe exceder de lo estrictamente necesario habida cuenta del objetivo perseguido, así como de las circunstancias que las justifican, sin perjuicio de que puedan ser renovadas si persiste la necesidad de proceder a dicha conservación (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 151).

83 En cuanto a la posibilidad de establecer algún criterio distintivo que no sea ni personal ni geográfico para efectuar una conservación selectiva de datos de tráfico y de localización, no puede excluirse que se tengan en cuenta otros criterios, objetivos y no discriminatorios, para garantizar que el alcance de una conservación selectiva se limite a lo estrictamente necesario y establecer un vínculo, al menos indirecto, entre los delitos graves y las personas cuyos datos va a conservarse. Ahora bien, dado que el artículo 15, apartado 1, de la Directiva 2002/58 se refiere a las medidas legales de los Estados miembros, incumbe a estos últimos y no al Tribunal de Justicia identificar tales criterios, partiendo de la base de que no puede tratarse de reinstaurar por esta vía una conservación generalizada e indiferenciada de los datos de tráfico y de localización.

84 En cualquier caso, como señaló el Abogado General Campos Sánchez-Bordona en el punto 50 de sus conclusiones en los asuntos acumulados SpaceNet y Telekom Deutschland (C-793/19 y C-794/19, EU:C:2021:939), la eventual existencia de dificultades para definir con precisión los casos y las condiciones en que pueda realizarse una conservación selectiva no

justifica que los Estados miembros, haciendo de la excepción una norma, establezcan una conservación generalizada e indiferenciada de datos de tráfico y de localización.

85 Por lo que respecta, a continuación, a la conservación rápida de los datos de tráfico y de localización tratados y almacenados por los proveedores de servicios de comunicaciones electrónicas de acuerdo con los artículos 5, 6 y 9 de la Directiva 2002/58 o con las medidas legales adoptadas en virtud del artículo 15, apartado 1, de dicha Directiva, procede recordar que tales datos, en principio, deben ser suprimidos o anonimizados, según los casos, al expirar los plazos legales en los que han de tener lugar, de conformidad con las disposiciones nacionales de transposición de la citada Directiva, su tratamiento y almacenamiento. No obstante, el Tribunal de Justicia ha declarado que, durante ese tratamiento y ese almacenamiento, pueden presentarse situaciones en las que surja la necesidad de conservar tales datos más allá de estos plazos para investigar delitos graves o atentados contra la seguridad nacional, tanto en la situación en que esos delitos o atentados ya hayan podido comprobarse como en aquella en la que su existencia pueda sospecharse fundadamente al término de un examen objetivo del conjunto de las circunstancias pertinentes (véase, en este sentido, 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 160 y 161).

86 En tal situación, habida cuenta de la conciliación necesaria de los derechos e intereses legítimos en juego a que se refieren los apartados 50 a 53 de la presente sentencia, los Estados miembros pueden establecer, en una normativa adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58, la posibilidad de requerir, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, a los proveedores de servicios de comunicaciones electrónicas para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan (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 163).

87 En la medida en que la finalidad de tal conservación rápida ya no se corresponde con las finalidades para las que los datos se recopilaron y conservaron en un principio y en que todo tratamiento de datos debe, con arreglo al artículo 8, apartado 2, de la Carta, efectuarse para fines concretos, los Estados miembros deben especificar en su normativa la finalidad para la que puede efectuarse la conservación rápida de los datos. Habida cuenta del carácter grave de la injerencia en los derechos fundamentales consagrados en

los artículos 7 y 8 de la Carta que puede suponer dicha conservación, únicamente pueden justificar esta injerencia la lucha contra la delincuencia grave y, *a fortiori*, la protección de la seguridad nacional, siempre que esa medida y el acceso a los datos así conservados no sobrepasen los límites de lo estrictamente necesario, como los enunciados en los apartados 164 a 167 de 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).

88 El Tribunal de Justicia ha indicado que una medida de conservación de esta naturaleza no debe limitarse a los datos de las personas identificadas previamente como representativas de una amenaza para la seguridad pública o la seguridad nacional del Estado miembro de que se trate o de personas de las que se sospecha que han cometido un delito grave o un atentado contra la seguridad nacional. En efecto, según el Tribunal de Justicia, respetando el marco establecido por 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, y habida cuenta de las consideraciones que figuran en el apartado 55 de la presente sentencia, dicha medida puede, según lo que elija el legislador y siempre dentro de los límites de lo estrictamente necesario, ampliarse a los datos de tráfico y de localización de personas distintas de las sospechosas de haber planeado o cometido un delito grave o un atentado contra la seguridad nacional, siempre que estos datos puedan, sobre la base de elementos objetivos y no discriminatorios, contribuir a la investigación de tal delito o de tal atentando contra la seguridad nacional, como los datos de la propia víctima o de su entorno social o profesional (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 165).

89 De esta manera, una medida legislativa puede autorizar el recurso a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan a la conservación rápida de los datos de tráfico y de localización, en particular, de las personas con las que haya estado en contacto una víctima al utilizar los medios de comunicaciones electrónicas de aquellos antes de que se produjera una amenaza grave para la seguridad pública o de que se cometiera un delito grave.

90 Según la jurisprudencia del Tribunal de Justicia recordada en el apartado 88 de la presente sentencia y en las mismas condiciones a las que se refiere dicho apartado, tal conservación rápida puede ampliarse igualmente a zonas geográficas determinadas tales como los lugares en que se cometió y se preparó el delito o el atentado contra la seguridad nacional de que se trate. Debe observarse que también pueden ser objeto de tal medida los datos de

tráfico y de localización relativos al lugar en el que una persona, víctima potencial de un delito grave, haya desaparecido, siempre que dicha medida y el acceso a los datos conservados de este modo respeten los límites de lo estrictamente necesario a efectos de la lucha contra la delincuencia grave o de la protección de la seguridad nacional enunciados en los apartados 164 a 167 de 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).

91 Por otra parte, debe señalarse que el artículo 15, apartado 1, de la Directiva 2002/58 no se opone a que las autoridades nacionales competentes ordenen una medida de conservación rápida ya en la primera fase de la investigación relativa a una amenaza grave para la seguridad pública o a un eventual delito grave, a saber, desde el momento en que esas autoridades puedan incoar tal investigación con arreglo a las disposiciones pertinentes del Derecho nacional.

92 En cuanto a la variedad de las medidas de conservación de datos de tráfico y de localización a que se refiere el apartado 67 de la presente sentencia, no puede obviarse que esas distintas medidas pueden aplicarse conjuntamente, según la elección del legislador nacional y siempre que se respeten los límites de lo estrictamente necesario. En tales condiciones, 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, tal como lo ha interpretado la jurisprudencia sentada en 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), no se opone a una combinación de esas medidas.

93 En cuarto y último lugar, se impone advertir que la proporcionalidad de las medidas adoptadas en virtud del artículo 15, apartado 1, de la Directiva 2002/58 requiere, según la reiterada jurisprudencia del Tribunal de Justicia a la que se hace referencia sumariamente en 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), la observancia no solo de los requisitos de aptitud y necesidad, sino también de la exigencia relativa al carácter proporcionado de esas medidas respecto del objetivo perseguido.

94 De este modo, procede recordar que, en el apartado 51 de su sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), el Tribunal de Justicia declaró que, si bien la lucha contra la delincuencia grave reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación, tal objetivo de interés

general, por fundamental que sea, no puede por sí solo justificar que se considere necesaria una medida de conservación generalizada e indiferenciada de los datos de tráfico y de localización como la establecida por la Directiva 2006/24.

95 De igual forma, el Tribunal de Justicia indicó, en el apartado 145 de 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), que ni siquiera las obligaciones positivas de los Estados miembros que pueden resultar, según el caso, de los artículos 3, 4 y 7 de la Carta y que se refieren, como se ha señalado en el apartado 49 de la presente sentencia, a la adopción de normas que permitan combatir eficazmente los delitos pueden tener por efecto justificar injerencias tan graves, como las que supone una normativa que establece una conservación de los datos de tráfico y de localización, en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta de prácticamente toda la población sin que los datos de las personas afectadas puedan guardar una relación, al menos indirecta, con el objetivo perseguido.

96 En la vista, el Gobierno danés sostuvo que las autoridades nacionales competentes deberían poder acceder, a efectos de la lucha contra la delincuencia grave, a los datos de tráfico y de localización que se hayan conservado de manera generalizada e indiferenciada, de acuerdo con la jurisprudencia dimanada de 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 135 a 139, para hacer frente a una amenaza grave contra la seguridad nacional que resulte real y actual o previsible.

97 Procede señalar de entrada que el hecho de autorizar el acceso, a efectos de la lucha contra la delincuencia grave, a datos de tráfico y de localización que se han conservado de manera generalizada e indiferenciada determina que dicho acceso va a depender de circunstancias ajenas a aquel objetivo, en función de que exista o no una amenaza grave para la seguridad nacional en el Estado miembro de que se trate, como la contemplada en el apartado anterior, mientras que, a la vista del objetivo de lucha contra la delincuencia grave que ha de justificar la conservación de esos datos y el acceso a ellos, no hay nada que justifique una diferencia de trato entre los Estados miembros.

98 Como ya ha declarado el Tribunal de Justicia, el acceso a los datos de tráfico y de localización conservados por los proveedores con arreglo a una medida adoptada de conformidad con el artículo 15, apartado 1, de la Directiva 2002/58, que debe efectuarse respetando los requisitos que se derivan de la jurisprudencia que ha interpretado la Directiva 2002/58, solo puede estar

justificado, en principio, por el objetivo de interés general para el que dicha conservación se impuso a estos proveedores. Solo cabría una solución diferente si la importancia del objetivo perseguido por el acceso fuera mayor que la del objetivo que justificó la conservación (véase, en este sentido, 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 165 y 166).

99 Pues bien, la argumentación del Gobierno danés alude a una situación en la que el objetivo de la solicitud de acceso en cuestión, a saber, la lucha contra la delincuencia grave, es de una importancia menor, en la jerarquía de los objetivos de interés general, que la del que justificó la conservación, a saber, la protección de la seguridad nacional. Autorizar, en tal situación, el acceso a los datos conservados sería contrario a la jerarquía de objetivos de interés general sugerida en el apartado anterior y en los apartados 53, 56, 57 y 59 de la presente sentencia.

100 Debe recalcarse en particular que, conforme a la jurisprudencia recordada en el apartado 65 de la presente sentencia, los datos de tráfico y de localización no pueden ser objeto de una conservación generalizada e indiferenciada a efectos de la lucha contra la delincuencia grave y, por tanto, estos mismos fines no pueden justificar un acceso a los referidos datos. Pues bien, si estos datos han sido excepcionalmente conservados de manera generalizada e indiferenciada, con fines de protección de la seguridad nacional contra una amenaza que resulta real y actual o previsible, en las condiciones mencionadas en el apartado 58 de la presente sentencia, las autoridades nacionales competentes en materia de investigación de los delitos no pueden acceder a dichos datos en el marco de un proceso penal, so pena de privar de todo efecto útil a la prohibición de efectuar tal conservación a efectos de la lucha contra la delincuencia grave, recordada en el apartado 65 antes citado.

101 Habida cuenta de todas las consideraciones que anteceden, procede responder a las cuestiones prejudiciales primera, segunda y cuarta 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 medidas legislativas que establezcan, con carácter preventivo, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización. En cambio, dicho artículo 15, apartado 1, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a medidas legislativas que, a efectos de la lucha

contra la delincuencia grave y de la prevención de amenazas graves contra la seguridad pública, establezcan:

– una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse;

– una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;

– una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y

– el recurso a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan esos proveedores de servicios,

siempre que dichas medidas garanticen, mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso.

Tercera cuestión prejudicial

102 Mediante su tercera cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si 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 en virtud de la cual el tratamiento centralizado de una solicitud de acceso a datos conservados, procedente de la Policía en el marco de la investigación y de la persecución de delitos graves, incumbe a un funcionario de la Policía asistido por una unidad integrada en este mismo cuerpo, con cierto grado de autonomía en el ejercicio de sus funciones y cuyas decisiones pueden ser objeto de un control jurisdiccional ulterior.

103 Con carácter preliminar, procede recordar que, si bien corresponde al Derecho nacional determinar las condiciones en las que los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos de que disponen, una normativa nacional debe establecer, para cumplir el requisito de proporcionalidad al que se ha hecho referencia en el apartado 54 de la presente sentencia, 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 contra los riesgos de abuso [véase, en este sentido, la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 48 y jurisprudencia citada].

104 En particular, una normativa nacional que regula el acceso de las autoridades competentes a los datos de tráfico y de localización conservados, adoptada al amparo del artículo 15, apartado 1, de la Directiva 2002/58, no puede limitarse a exigir que el acceso de las autoridades a los datos responda a la finalidad perseguida por dicha normativa, sino que debe establecer también los requisitos materiales y procedimentales que regulen la referida utilización [sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 49 y jurisprudencia citada].

105 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 en cuestión. A este respecto, en principio solo podrá concederse un acceso de este tipo 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. No obstante, en situaciones particulares, como aquellas en las que intereses vitales de la seguridad nacional, la defensa o la seguridad pública estén 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 [sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de

acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 50 y jurisprudencia citada].

106 Para garantizar en la práctica el íntegro cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados se supedite a un control previo efectuado bien por un órgano jurisdiccional, bien por un órgano administrativo independiente y que la decisión de este órgano jurisdiccional o administrativo se dicte a raíz de una solicitud motivada de dichas autoridades presentada, en particular, en el marco de procedimientos de prevención, descubrimiento y persecución de delitos [sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 51 y jurisprudencia citada].

107 Este control previo requiere, entre otras cosas, que el órgano jurisdiccional o administrativo encargado de efectuarlo disponga de todas las atribuciones y presente todas las garantías necesarias para conciliar los diferentes intereses legítimos y derechos de que se trate. En el caso concreto de una investigación penal, tal control exige que ese órgano jurisdiccional o administrativo esté en condiciones de ponderar adecuadamente, por una parte, los intereses legítimos relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales que asisten a las personas a cuyos datos se pretende acceder [sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 52].

108 Cuando dicho control no lo lleve a cabo un órgano jurisdiccional, sino un órgano administrativo independiente, este último debe gozar de un estatuto que le permita actuar en el ejercicio de sus funciones con objetividad e imparcialidad y, para ello, ha de estar a resguardo de toda influencia externa. De esta manera, el requisito de independencia que debe cumplir el órgano que ejerce el control previo obliga a que este tenga la condición de tercero respecto del órgano que solicita el acceso a los datos, de modo que el primero pueda ejercer ese control con objetividad e imparcialidad, y a resguardo de toda influencia externa. En particular, en el ámbito penal, el requisito de independencia implica que la autoridad que ejerce ese control previo, por una parte, no esté implicada en la realización de la investigación penal de que se trate y, por otra parte, que tenga una posición neutral frente a las partes del procedimiento penal [véase, en este sentido, la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las

comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartados 53 y 54].

109 El Tribunal de Justicia ha considerado, pues, que no puede conferirse a un Ministerio Fiscal que dirige el procedimiento de investigación y ejerce, en su caso, la acusación pública la calidad de tercero con respecto a los intereses legítimos en cuestión, toda vez que su función no es resolver con total independencia un litigio, sino someterlo, en su caso, al órgano jurisdiccional competente, como parte en el proceso que ejerce la acusación penal. Por consiguiente, el Ministerio Fiscal no puede llevar a cabo el control previo de las solicitudes de acceso a los datos conservados [véase, en este sentido, la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartados 55 y 57].

110 Finalmente, el control independiente exigido con arreglo al artículo 15, apartado 1, de la Directiva 2002/58 debe realizarse antes de cualquier acceso a los datos en cuestión, salvo en caso de urgencia debidamente justificada, supuesto en el cual el control debe efectuarse en breve plazo. En efecto, un control ulterior sería opuesto al objetivo del control previo, que consiste en impedir que se autorice un acceso a los datos en cuestión que exceda de los límites de lo estrictamente necesario [véanse, en este sentido, las sentencias 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 189, y de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 58].

111 En el presente asunto, de la petición de decisión prejudicial se deduce, en primer término, que la Ley de 2011 atribuye a un funcionario de la Policía, de rango no inferior al de comisario, la competencia para ejercer el control previo de una solicitud de acceso a los datos procedente de los servicios de investigación policial y para solicitar a los proveedores de servicios de comunicaciones electrónicas que le comuniquen los datos que conservan. En la medida en que dicho funcionario no tiene la calidad de tercero con respecto a esos servicios, no cumple las exigencias de independencia e imparcialidad mencionadas en el apartado 108 de la presente sentencia, pese a la circunstancia de estar asistido en esa función por una unidad de la Policía, en este caso la TLU, que goza de cierto grado de autonomía en el ejercicio de sus funciones.

112 A continuación, si bien es cierto que la Ley de 2011 establece mecanismos de control *a posteriori* de la decisión del funcionario de la Policía competente

por la vía de un procedimiento de reclamación y de un procedimiento ante un juez encargado de verificar la aplicación de las disposiciones de dicha Ley, de la jurisprudencia recordada en el apartado 110 de la presente sentencia se desprende que la exigencia mencionada en el apartado 106 de la presente sentencia relativa a un control independiente y, salvo urgencia debidamente justificada, de carácter previo no puede ser sustituida por un control ejercido *a posteriori*.

113 Por último, la Ley de 2011 no establece criterios objetivos que definan con precisión las condiciones y las circunstancias en que debe concederse a las autoridades nacionales el acceso a los datos, ya que el funcionario de la Policía encargado de tramitar las solicitudes de acceso a los datos conservados es el único competente, como confirmó Irlanda en la vista, para apreciar las sospechas que recaen sobre las personas afectadas y la necesidad de acceder a los datos relativos a estas últimas.

114 Por consiguiente, procede responder a la tercera cuestión prejudicial 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 en virtud de la cual el tratamiento centralizado de una solicitud de acceso a datos conservados por los proveedores de servicios de comunicaciones electrónicas, procedente de la Policía en el marco de la investigación y de la persecución de delitos graves, incumbe a un funcionario de la Policía asistido por una unidad integrada en este mismo cuerpo, con cierto grado de autonomía en el ejercicio de sus funciones y cuyas decisiones pueden ser objeto de un control jurisdiccional ulterior.

Cuestiones prejudiciales quinta y sexta

115 Mediante sus cuestiones prejudiciales quinta y sexta, que deben ser examinadas conjuntamente, el órgano jurisdiccional remitente desea que se dilucide, en esencia, si el Derecho de la Unión debe interpretarse en el sentido de que un órgano jurisdiccional nacional puede limitar en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, en virtud del Derecho nacional, con respecto a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en razón de la incompatibilidad de dicha normativa con el artículo 15, apartado 1, de la Directiva 2002/58 a la vista de la Carta.

116 De la información facilitada por el órgano jurisdiccional remitente se deduce que la normativa nacional controvertida en el litigio principal, a saber, la Ley de 2011, se adoptó con el fin de transponer al Derecho nacional la Directiva 2006/24, la cual fue posteriormente declarada inválida por el Tribunal de Justicia en su sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238).

117 Además, el órgano jurisdiccional remitente señala que, si bien incumbe al juez penal el examen de la admisibilidad de las pruebas basadas en datos conservados en virtud de la Ley de 2011 e invocadas contra G. D. en el marco del proceso penal, a él le corresponde, no obstante, en el marco del procedimiento civil, resolver sobre la validez de las disposiciones controvertidas de dicha Ley y sobre los efectos temporales de una declaración de invalidez que afecte a estas. Así, aunque la única cuestión que se suscita ante el órgano jurisdiccional remitente es la de la validez de las disposiciones de la Ley de 2011, dicho órgano jurisdiccional considera no obstante necesario preguntar al Tribunal de Justicia sobre la incidencia de una eventual declaración de invalidez en la admisibilidad de las pruebas obtenidas mediante la conservación generalizada e indiferenciada de los datos efectuada al amparo de la citada Ley.

118 Con carácter preliminar, conviene recordar que el principio de primacía del Derecho de la Unión supone la prevalencia de este ordenamiento sobre el Derecho de los Estados miembros. Dicho principio obliga a todos los órganos e instituciones de los Estados miembros, por tanto, a garantizar la plena eficacia de las diferentes disposiciones del Derecho de la Unión, sin que el Derecho de los Estados miembros pueda oponerse al efecto reconocido a las referidas disposiciones en el territorio de estos Estados. En virtud del referido principio, cuando no resulte posible interpretar la normativa nacional conforme a las exigencias del Derecho de la Unión, el juez nacional encargado de aplicar, en el ámbito de su competencia, las disposiciones del Derecho de la Unión tendrá la obligación de garantizar la plena eficacia de estas, dejando inaplicada si fuera necesario, y por su propia iniciativa, cualquier disposición contraria de la legislación nacional, aun posterior, sin que deba solicitar o esperar su previa eliminación por vía legislativa o mediante cualquier otro procedimiento constitucional [véanse, en este sentido, las sentencias de 15 de julio de 1964, Costa, 6/64, EU:C:1964:66, pp. 105 y 106; de 19 de noviembre de 2019, A. K. y otros (Independencia de la Sala Disciplinaria del Tribunal Supremo), C-585/18, C-624/18 y C-625/18, EU:C:2019:982, apartados 157, 158 y 160, así como 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 214 y 215].

119 Solo el Tribunal de Justicia puede, con carácter excepcional y en atención a consideraciones imperiosas de seguridad jurídica, suspender provisionalmente el efecto de exclusión que ejerce una norma de la Unión sobre el Derecho nacional contrario a ella. Dicha limitación temporal de los efectos de la interpretación de este Derecho dada por el Tribunal de Justicia solo puede admitirse en la propia sentencia que resuelve sobre la interpretación solicitada. Se estaría actuando en menoscabo de la primacía y de la aplicación uniforme del Derecho de la Unión si los órganos jurisdiccionales nacionales estuvieran facultados para otorgar primacía a las normas nacionales contrarias a este último ordenamiento, aunque fuera con carácter provisional (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 216 y 217 y jurisprudencia citada).

120 Es cierto que el Tribunal de Justicia ha considerado, en un asunto relativo a la legalidad de unas medidas adoptadas incumpliendo la obligación impuesta por el Derecho de la Unión de efectuar una evaluación previa de las repercusiones de un proyecto sobre el medio ambiente y sobre un lugar protegido, que un órgano jurisdiccional nacional puede, si el Derecho interno se lo permite, mantener excepcionalmente los efectos de tales medidas si ese mantenimiento está justificado por consideraciones imperiosas relacionadas con la necesidad de evitar una amenaza real y grave de corte del suministro eléctrico del Estado miembro afectado a la que no podría hacerse frente por otros medios y otras alternativas, en particular en el marco del mercado interior. Dicho mantenimiento solo podrá extenderse el tiempo estrictamente necesario para corregir la referida ilegalidad (véase, en este sentido, la sentencia de 29 de julio de 2019, Inter-Environnement Wallonie y Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, apartados 175, 176, 179 y 181).

121 Ahora bien, contrariamente al incumplimiento de una obligación procedimental como la evaluación previa de las repercusiones de un proyecto, que se inscribe en el ámbito específico de la protección del medio ambiente, la infracción 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, no puede ser objeto de una regularización mediante un procedimiento comparable al mencionado en el apartado anterior (véase, en este sentido, 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, apartado 219).

122 En efecto, el mantenimiento de los efectos de una normativa nacional como la Ley de 2011 significaría que dicha normativa sigue imponiendo a los

proveedores de servicios de comunicaciones electrónicas obligaciones que son contrarias al Derecho de la Unión y que suponen injerencias graves en los derechos fundamentales de las personas cuyos datos se han conservado (véase, por analogía, 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, apartado 219).

123 Por lo tanto, no le es lícito al órgano jurisdiccional remitente limitar en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, con arreglo al Derecho nacional, con respecto a la normativa nacional controvertida en el litigio principal (véase, por analogía, 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, apartado 220).

124 A este respecto, como señaló en esencia el Abogado General en el punto 75 de sus conclusiones, la circunstancia de que esa normativa nacional se adoptara con objeto de transponer la Directiva 2006/24 al Derecho nacional carece de pertinencia toda vez que, invalidada dicha Directiva por el Tribunal de Justicia con efectos que se retrotraen a la fecha de su entrada en vigor (véase, en este sentido, la sentencia de 8 de febrero de 1996, FMC y otros, C-212/94, EU:C:1996:40, apartado 55), el órgano jurisdiccional remitente debe apreciar la validez de esa normativa nacional a la luz de la Directiva 2002/58 y de la Carta tal como las interpreta el Tribunal de Justicia.

125 En particular, con relación a la interpretación de la Directiva 2002/58 y de la Carta efectuada por el Tribunal de Justicia en sus sentencias, entre otras, de 21 de diciembre de 2016 Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), 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), conviene recordar que, según reiterada jurisprudencia, la interpretación que el Tribunal de Justicia efectúa, en el ejercicio de la competencia que le confiere el artículo 267 TFUE, de una norma de Derecho de la Unión aclara y precisa el significado y el alcance de dicha norma, tal como debe o habría debido ser entendida y aplicada desde el momento de su entrada en vigor. De ello resulta que la norma que ha sido interpretada puede y debe ser aplicada por el juez a las relaciones jurídicas nacidas y constituidas antes de que se haya pronunciado la sentencia que resuelva sobre la petición de interpretación si, además, se cumplen los requisitos que permiten someter a los órganos jurisdiccionales competentes un litigio relativo a la aplicación de dicha norma (sentencia de 16 de septiembre de 2020, Romenergo y Aris Capital, C-339/19, EU:C:2020:709, apartado 47 y jurisprudencia citada).

126 A este respecto, debe advertirse que los efectos de la interpretación en cuestión no se limitaron en el tiempo en las sentencias de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), 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), de suerte que, conforme a la jurisprudencia recordada en el apartado 119 de la presente sentencia, una sentencia del Tribunal de Justicia posterior a estas no puede establecer tal limitación.

127 Por último, en cuanto a la incidencia de la declaración de la eventual incompatibilidad de la Ley de 2011 con la Directiva 2002/58, a la vista de la Carta, en la admisibilidad de las pruebas presentadas contra G. D. en el proceso penal, basta con remitirse a la jurisprudencia pertinente del Tribunal de Justicia, en particular a los principios recordados en los apartados 41 a 44 de la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, EU:C:2021:152), de la que se desprende que esa admisibilidad se rige, en virtud del principio de autonomía procesal de los Estados miembros, por el Derecho nacional, sin perjuicio del respeto en particular de los principios de equivalencia y efectividad.

128 Habida cuenta de las consideraciones anteriores, procede responder a las cuestiones prejudiciales quinta y sexta que el Derecho de la Unión debe interpretarse en el sentido de que se opone a que un órgano jurisdiccional nacional limite en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, en virtud del Derecho nacional, con respecto a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en razón de la incompatibilidad de esa normativa con el artículo 15, apartado 1, de la Directiva 2002/58 a la vista de la Carta. Conforme al principio de autonomía procesal de los Estados miembros, la admisibilidad de las pruebas obtenidas mediante tal conservación se rige por el Derecho nacional, sin perjuicio del respeto en particular de los principios de equivalencia y efectividad.

Costas

129 Dado que el procedimiento tiene, para las partes del litigio principal, el carácter de un incidente promovido ante el órgano jurisdiccional nacional, 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) **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 medidas legislativas que establezcan, con carácter preventivo, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización. En cambio, dicho artículo 15, apartado 1, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales, no se opone a medidas legislativas que, a efectos de la lucha contra la delincuencia grave y de la prevención de amenazas graves contra la seguridad pública, establezcan:**

   – **una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse;**

   – **una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;**

   – **una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y**

– **el recurso a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan estos proveedores de servicios,**

siempre que dichas medidas garanticen, mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso.

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 en virtud de la cual el tratamiento centralizado de una solicitud de acceso a datos conservados por los proveedores de servicios de comunicaciones electrónicas, procedente de la Policía en el marco de la investigación y la persecución de delitos graves, corresponde a un funcionario de la Policía asistido por una unidad integrada en este mismo cuerpo, con cierto grado de autonomía en el ejercicio de sus funciones y cuyas decisiones pueden ser objeto de un control jurisdiccional ulterior.

3) El Derecho de la Unión debe interpretarse en el sentido de que se opone a que un órgano jurisdiccional nacional limite en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, en virtud del Derecho nacional, con respecto a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en razón de la incompatibilidad de esa normativa con el artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, a la vista de la Carta de los Derechos Fundamentales. Conforme al principio de autonomía procesal de los Estados miembros, la admisibilidad de las pruebas obtenidas mediante tal conservación se rige por el Derecho nacional, sin perjuicio del respeto en particular de los principios de equivalencia y efectividad.

Firmas