Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 6 de octubre de 2020 *

[Texto rectificado mediante auto de 16 de noviembre de 2020]

Índice

Marco jurídico 7
Derecho de la Unión 7
Directiva 95/46/CE 7
Directiva 97/66/CE 7
Directiva 2000/31 8
Directiva 2002/21/CE 9
Directiva 2002/58 10
Reglamento 2016/679 14
Derecho francés 18
Código de Seguridad Interior 18
CPCE 23
Ley n.º 2004-575, de 21 de junio de 2004, relativa a la Confianza en la Economía Digital 25
Decreto n.º 2011-219 25
Derecho belga 27
Litigios principales y cuestiones prejudiciales 29
Asunto C-511/18 29
Asunto C-512/18 32

* Lengua de procedimiento: francés.

Asunto C-520/18 33

Sobre el procedimiento ante el Tribunal de Justicia 35

Sobre las cuestiones prejudiciales 35

Primeras cuestiones prejudiciales planteadas en los asuntos C-511/18 y C-512/18 y sobre las cuestiones prejudiciales primera y segunda planteadas en el asunto C-520/18 35

Observaciones preliminares 35

Sobre el ámbito de aplicación de la Directiva 2002/58 37

Sobre la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 40

– Sobre las medidas legislativas que establecen la conservación preventiva de los datos de tráfico y de los datos de localización para proteger la seguridad nacional 45

– Sobre las medidas legislativas que establecen la conservación preventiva de los datos de tráfico y de los datos de localización a efectos de la lucha contra la delincuencia y de la protección de la seguridad pública 46

– Sobre las medidas legislativas que establecen la conservación preventiva de las direcciones IP y de los datos relativos a la identidad civil a efectos de la lucha contra la delincuencia y de la protección de la seguridad pública 48

– Sobre las medidas legislativas que establecen la conservación rápida de los datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave 50

Cuestiones prejudiciales segunda y tercera planteadas en el asunto C-511/18 53

Sobre el análisis automatizado de los datos de tráfico y de localización 53

Sobre la recopilación en tiempo real de los datos de tráfico y de localización 55

Sobre la información de las personas cuyos datos han sido recopilados o analizados 57

Segunda cuestión prejudicial planteada en el asunto C-512/18 58

Tercera cuestión prejudicial planteada en el asunto C-520/18 61

Costas 64

«Procedimiento prejudicial — Tratamiento de datos de carácter personal en el sector de las comunicaciones electrónicas — Proveedores de servicios de comunicaciones electrónicas — Proveedores de servicios de almacenamiento y proveedores de acceso a Internet — Conservación generalizada e indiferenciada de datos de tráfico y de localización — Análisis automatizado de datos — Acceso en tiempo real a los datos — Protección de la seguridad nacional y lucha contra el terrorismo — Lucha contra la delincuencia — Directiva 2002/58/CE — Ámbito de aplicación — Artículo 1, apartado 3, y 3 — Confidencialidad de las comunicaciones

electrónicas — Protección — Artículo 5 y 15, apartado 1 — Directiva 2000/31/CE — Ámbito de aplicación — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 4, 6 a 8 y 11 y artículo 52, apartado 1 — Artículo 4 TUE, apartado 2»

En los asuntos acumulados C-511/18, C-512/18 y C-520/18,

que tienen por objeto sendas peticiones de decisión prejudicial planteadas, con arreglo al artículo 267 TFUE, por el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia), mediante resoluciones de 26 de julio de 2018, recibidas en el Tribunal de Justicia el 3 de agosto de 2018 (C-511/18 y C-512/18), y por la Cour constitutionnelle (Tribunal Constitucional, Bélgica), mediante resolución de 19 de julio de 2018, recibida en el Tribunal de Justicia el 2 de agosto de 2018 (C-520/18), en los procedimientos entre

La Quadrature du Net (C-511/18 y C-512/18),

French Data Network (C-511/18 y C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 y C-512/18),

Igwan.net (C-511/18)

y

Premier ministre (C-511/18 y C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 y C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18),

con intervención de:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18)

y

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

y

Conseil des ministres,

con intervención de:

Child Focus (C-520/18),

EL TRIBUNAL DE JUSTICIA (Gran Sala),

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

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

Secretaria: Sra. C. Strömholm, administradora;

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

consideradas las observaciones presentadas:

– en nombre de La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net y el Center for Democracy and Technology, por el Sr. A. Fitzjean Ò Cobhthaigh, avocat;

– en nombre de French Data Network, por el Sr. Y. Padova, avocat;

– en nombre de Privacy International, por el Sr. H. Roy, avocat;

– en nombre del Ordre des barreaux francophones et germanophone, por los Sres. E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart y J.-F. Henrotte, avocats;

– en nombre de la Académie Fiscale ASBL y UA, por el Sr. J.-P. Riquet;

– en nombre de la Liga voor Mensenrechten ASBL, por el Sr. J. Vander Velpen, avocat;

– en nombre de la Ligue des Droits de l'Homme ASBL, por los Sres. R. Jespers y J. Fermon, avocats;

– en nombre de VZ, WY y XX, por el Sr. D. Pattyn, avocat;

– en nombre de Child Focus, por los Sres. N. Buisseret, K. De Meester y J. Van Cauter, avocats;

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

– en nombre del Gobierno belga, por los Sres. J.-C. Halleux y P. Cottin y por la Sra. C. Pochet, en calidad de agentes, asistidos por los Sres. J. Vanpraet, Y. Peeters, S. Depré y E. de Lophem, avocats;

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

– en nombre del Gobierno danés, inicialmente por el Sr. J. Nymann-Lindegren y por las Sras. M. Wolff y P. Ngo, y posteriormente por el Sr. J. Nymann-Lindegren y la Sra. M. Wolff, en calidad de agentes;

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

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

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

– en nombre del Gobierno español, inicialmente por los Sres. L. Aguilera Ruiz y A. Rubio González, y posteriormente por el Sr. L. Aguilera Ruiz, en calidad de agente;

– en nombre del Gobierno chipriota, por la Sra. E. Neofytou, en calidad de agente;

– en nombre del Gobierno letón, por la Sra. V. Soņeca, en calidad de agente;

– en nombre del Gobierno húngaro, inicialmente por el Sr. M. Z. Fehér y la Sra. Z. Wagner, y posteriormente por el Sr. M. Z. Fehér, en calidad de agente;

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

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

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

– en nombre del Gobierno del Reino Unido, por el Sr. S. Brandon, en calidad de agente, asistido por el Sr. G. Facenna, QC, y por el Sr. C. Knight, Barrister;

– [guion suprimido mediante auto de 16 de noviembre de 2020];

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

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

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

dicta la siguiente

Sentencia

1 Las peticiones de decisión prejudicial tienen por objeto la interpretación, por una parte, 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»), y, por otra parte, de los artículos 12 a 15 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO 2000, L 178, p. 1), en relación con los artículos 4, 6 a 8 y 11 y con el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta») y con el artículo 4 TUE, apartado 2.

2 La petición en el asunto C-511/18 se ha presentado en el contexto de varios litigios entre, por un lado, La Quadrature du Net, French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs e Igwan.net y, por otro, el Premier ministre (Primer Ministro, Francia), el Garde des Sceaux, ministre de la Justice (Ministro de Justicia, Francia), el ministre de l'Intérieur (Ministro del Interior, Francia) y el ministre des Armées (Ministro de Defensa, Francia), relativos a la legalidad del décret n.º 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (Decreto n.º 2015-1185, de 28 de septiembre de 2015, de Designación de Servicios Especializados de Información) (JORF de 29 de septiembre de 2015, texto 1 de 97; en lo sucesivo, «Decreto n.º 2015-1185»); del décret n.º 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (Decreto n.º 2015-1211, de 1 de octubre de 2015, relativo a los recursos sobre la aplicación de técnicas de información sujetas a autorización y ficheros que afecten a la seguridad del Estado) (JORF de 2 de octubre de 2015, texto 7 de 108; en lo sucesivo, «Decreto n.º 2015-1211»); del décret n.º 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure (Decreto n.º 2015-1639, de 11 de diciembre de 2015, relativo a la designación de servicios, distintos de los servicios especializados de información, autorizados a utilizar las técnicas mencionadas en el título V del libro VIII del Código de Seguridad Interior) (JORF de 12 de diciembre de 2015, texto 28 de 127; en lo sucesivo, «Decreto n.º 2015-1639»), y del décret n.º 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (Decreto n.º 2016-67, de 29 de enero de 2016, relativo a las Técnicas de Recopilación de Información) (JORF de 31 de enero de 2016, texto 2 de 113; en lo sucesivo, «Decreto n.º 2016-67»).

3 La petición en el asunto C-512/18 se ha presentado en el contexto de varios litigios entre, por un lado, French Data Network, La Quadrature du Net y la Fédération des fournisseurs d'accès à Internet associatifs y, por otro, el Primer Ministro de Francia y el Ministro de Justicia francés, relativos a la legalidad del artículo R. 10-13 del code des postes et des communications électroniques (Código de Correos y Comunicaciones Electrónicas; en lo sucesivo, «CPCE») y del décret n.º 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Decreto n.º 2011-219, de 25 de febrero de 2011, sobre la conservación de los datos que permitan la identificación de toda persona que haya contribuido a la creación de un contenido ofrecido en línea) (JORF de 1 de marzo de 2011, texto 32 de 170; en lo sucesivo, «Decreto n.º 2011-219»).

4 La petición en el asunto C-520/18 se ha presentado en el contexto de varios litigios entre, por un lado, el Ordre des barreaux francophones et germanophone, la Académie Fiscale ASBL, UA, la Liga voor Mensenrechten ASBL, la Ligue des Droits de l'Homme ASBL, VZ, WY y XX y, por otro, el Conseil des ministres (Consejo de Ministros, Bélgica), relativos a la legalidad de la loi du 29 mai 2016 relative

à la collecte et à la conservation des données dans le secteur des communications électroniques (Ley de 29 de mayo de 2016 de Recogida y Conservación de Datos en el Sector de las Comunicaciones Electrónicas) (*Moniteur belge* de 18 de julio de 2016, p. 44717; en lo sucesivo, «Ley de 29 de mayo de 2016»).

Marco jurídico

Derecho de la Unión

Directiva 95/46/CE

5 La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31), fue derogada, con efectos a partir del 25 de mayo de 2018, por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46 (DO 2016, L 119, p. 1). El artículo 3, apartado 2, de la Directiva 95/46 establecía que:

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

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

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

6 El artículo 22 de la Directiva 95/46, que figura en su capítulo III, titulado «Recursos judiciales, responsabilidad y sanciones», tenía el siguiente tenor:

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

Directiva 97/66/CE

7 Con arreglo al artículo 5 de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (DO 1997, L 24, p. 1), titulado «Confidencialidad de las comunicaciones»:

«1. Los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. En particular, prohibirán la escucha, la grabación, el

almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente, de conformidad con el apartado 1 del artículo 14.

2. El apartado 1 no se aplicará a las grabaciones legalmente autorizadas de comunicaciones en el marco de una práctica comercial lícita destinada a aportar pruebas de una transacción comercial o de cualquier otra comunicación comercial.»

Directiva 2000/31

8 A tenor de lo dispuesto en los considerandos 14 y 15 de la Directiva 2000/31:

«(14) La protección de las personas con respecto al tratamiento de datos de carácter personal se rige únicamente por la Directiva [95/46] y la Directiva [97/66], que son enteramente aplicables a los servicios de la sociedad de la información. Dichas Directivas establecen ya un marco jurídico comunitario en materia de datos personales y, por tanto, no es necesario abordar este aspecto en la presente Directiva para garantizar el correcto funcionamiento del mercado interior, en particular la libre circulación de datos personales entre Estados miembros. La aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios, la presente Directiva no puede evitar el uso anónimo de redes abiertas como Internet.

(15) La confidencialidad de las comunicaciones queda garantizada por el artículo 5 de la Directiva [97/66]; basándose en dicha Directiva, los Estados miembros deben prohibir cualquier forma de interceptar o vigilar esas comunicaciones por parte de cualquier persona que no sea su remitente o su destinatario salvo que esté legalmente autorizada.»

9 El artículo 1 de la Directiva 2000/31 está redactado en los siguientes términos:

«1. El objetivo de la presente Directiva es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

2. En la medida en que resulte necesario para alcanzar el objetivo enunciado en el apartado 1 mediante la presente Directiva, se aproximarán entre sí determinadas disposiciones nacionales aplicables a los servicios de la sociedad de la información relativas al mercado interior, el establecimiento de los prestadores de servicios, las comunicaciones comerciales, los contratos por vía electrónica, la responsabilidad de los intermediarios, los códigos de conducta, los acuerdos extrajudiciales para la solución de litigios, los recursos judiciales y la cooperación entre Estados miembros.

3. La presente Directiva completará el ordenamiento jurídico comunitario aplicable a los servicios de la sociedad de la información, sin perjuicio del nivel de protección, en particular, de la salud pública y de los intereses del consumidor, fijados tanto en los instrumentos comunitarios como en las legislaciones nacionales que los desarrollan, en la medida en que nos restrinjan la libertad de prestar servicios de la sociedad de la información.

[…]

5. La presente Directiva no se aplicará:

[…]

b) a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas [95/46] y [97/66];

[…]».

10 El artículo 2 de la Directiva 2000/31 establece lo siguiente:

«A efectos de la presente Directiva, se entenderá por:

a) "servicios de la sociedad de la información": servicios en el sentido del apartado 2 del artículo 1 de la Directiva 98/34/CE [del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas (DO 1998, L 204, p. 37)], modificada por la Directiva 98/48/CE [del Parlamento Europeo y del Consejo, de 20 de julio de 1998 (DO 1998, L 217, p. 18)];

[…]».

11 El artículo 15 de la Directiva 2000/31 dispone que:

«1. Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14.

2. Los Estados miembros podrán establecer obligaciones tendentes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o la obligación de comunicar a las autoridades competentes, a solicitud de estas, información que les permita identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento.»

Directiva 2002/21/CE

12 Con arreglo a lo dispuesto en el considerando 10 de 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):

«La definición de "servicio de la sociedad de la información" que figura en el artículo 1 de la Directiva [98/34, en su versión modificada por la Directiva 98/48], abarca una amplia gama de actividades económicas que tienen lugar en línea; la mayoría de estas actividades no están cubiertas por la presente Directiva por no tratarse total o principalmente del transporte de señales en redes de comunicaciones electrónicas. La telefonía vocal y los servicios de correo electrónico están cubiertos por la presente Directiva. Una misma empresa, por ejemplo un proveedor de servicios de Internet, puede ofrecer tanto un servicio de comunicaciones electrónicas, tal como el acceso a Internet, como servicios no cubiertos por la presente Directiva, tales como el suministro de contenidos en forma de páginas de Internet.»

13 El artículo 2 de la Directiva 2002/21 prevé que:

«A efectos de la presente Directiva, se entenderá por:

[…]

c) “servicio de comunicaciones electrónicas”: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos asimismo los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva [98/34] que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas;

[…]».

Directiva 2002/58

14 Los considerandos 2, 6, 7, 11, 22, 26 y 30 de la Directiva 2002/58 tienen el siguiente tenor:

«(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 dicha Carta.

[…]

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

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

[…]

(11) Al igual que la Directiva [95/46], la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho [de la Unión]. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, [firmado en Roma el 4 de noviembre de 1950,] según la interpretación que se hace de este en las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

[…]

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

[…]

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

[…].

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

15 El artículo 1 de la Directiva 2002/58, titulado «Ámbito de aplicación y objetivo», está redactado en los siguientes términos:

«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.»

16 Con arreglo al 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].

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;

[…]».

17 A tenor de lo dispuesto en el artículo 3 de la Directiva 2002/58, titulado «Servicios afectados»:

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

18 En virtud del artículo 5 de la Directiva 2002/58, titulado «Confidencialidad de las comunicaciones»:

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

[…]

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

red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario.»

19 El artículo 6 de la Directiva 2002/58, titulado «Datos de tráfico», prevé que:

«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.»

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

«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. […]»

21 El artículo 15 de la citada Directiva, titulado «Aplicación de determinadas disposiciones de la Directiva [95/46]», prevé que:

«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.

[…]

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

[…]»

Reglamento 2016/679

22 Con arreglo al considerando 10 del Reglamento 2016/679:

«Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. […]»

23 A tenor de lo dispuesto en el artículo 2 de dicho Reglamento:

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

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

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

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

[…]

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

[…]

4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva [2000/31], en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.»

24 El artículo 4 de dicho Reglamento prevé que:

«A efectos del presente Reglamento se entenderá por:

1) "datos personales": toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

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

[…]».

25 De conformidad con el artículo 5 del Reglamento 2016/679:

«1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia");

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales ("limitación de la finalidad");

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos");

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan ("exactitud");

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ("limitación del plazo de conservación");

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad").

[…]»

26 El artículo 6 de dicho Reglamento está redactado en los siguientes términos:

«1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

[…]

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

[…]

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica […] Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

[…]»

27 En virtud del artículo 23 del citado Reglamento:

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

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

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

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

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

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

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

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

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate;

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.»

28 Con arreglo al artículo 79, apartado 1, de dicho Reglamento:

«Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.»

29 A tenor de lo dispuesto en el artículo 94 del Reglamento 2016/679:

«1. Queda derogada la Directiva [95/46] con efecto a partir del 25 de mayo de 2018.

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

30 El artículo 95 de dicho Reglamento dispone que:

«El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva [2002/58].»

Derecho francés

Código de Seguridad Interior

31 El libro VIII de la parte legislativa del code de la sécurité intérieure (Código de Seguridad Interior; en lo sucesivo, «CSI»), prevé, en sus artículos L. 801-1 a L. 898-1, normas relativas a la información.

32 El artículo L. 811-3 del CSI dispone que:

«Únicamente a efectos del ejercicio de sus respectivas misiones, los servicios especializados de información pueden utilizar las técnicas mencionadas en el título V del presente libro para recopilar información relativa a la defensa y a la promoción de los intereses fundamentales de la nación que se exponen a continuación:

1.º Independencia nacional, integridad del territorio y defensa nacional.

2.º Principales intereses de la política exterior, ejecución de los compromisos adquiridos por Francia a nivel europeo e internacional y prevención de cualquier injerencia exterior.

3.º Principales intereses económicos, industriales y científicos de Francia.

4.º Prevención del terrorismo.

5.º Prevención:
a) de los atentados contra la forma republicana de las instituciones;
b) de las acciones dirigidas al mantenimiento o al restablecimiento de las agrupaciones disueltas con arreglo al artículo L. 212-1;
c) de los actos de violencia colectiva que puedan alterar gravemente el orden público.

6.º Prevención de la criminalidad y de la delincuencia organizadas.

7.º Prevención de la proliferación de armas de destrucción masiva.»

33 Con arreglo al artículo L. 811-4 del CSI:

«Mediante decreto consultado al Conseil d'État (Consejo de Estado, Francia) adoptado previo dictamen de la Commission nationale de contrôle des techniques de renseignement (Comisión Nacional de Control de las Técnicas de Información, Francia), se designarán los servicios, distintos de los servicios especializados de información, incluidos en el ámbito de competencia de los Ministros de Defensa, del Interior y de Justicia, así como de los Ministros de Economía, Presupuestos o Aduanas, que pueden estar autorizados a utilizar las técnicas mencionadas en el título V del presente libro en las condiciones previstas en el mismo. Se especificarán, respecto de cada servicio, los fines mencionados en el artículo L. 811-3 y las técnicas que podrán ser autorizadas.»

34 A tenor de lo dispuesto en el artículo L. 821-1, párrafo primero, del CSI:

«Requerirá autorización previa del Primer Ministro, concedida previo dictamen de la Comisión Nacional de Control de las Técnicas de Información, la aplicación en el territorio nacional de las técnicas de recopilación de información mencionadas en los capítulos I a IV del título V del presente libro.»

35 El artículo L. 821-2 del CSI prevé que:

«La autorización mencionada en el artículo L. 821-1 se concederá previa solicitud escrita y motivada del Ministro de Defensa, del Ministerio del Interior, del Ministro de Justicia o de los Ministros de Economía, Presupuestos o Aduanas. Cada Ministro solo podrá delegar esta facultad individualmente a colaboradores directos autorizados a acceder a información confidencial en materia de defensa nacional.

La solicitud especificará:

1.º la(s) técnica(s) que se ha(n) de aplicar;

2.º el servicio para el que se presenta;

3.º la(s) finalidad(es) perseguida(s);

4.º la motivación de las medidas;

5.º la vigencia de la autorización;

6.º la(s) persona(s), el/los lugar(es) o vehículos en cuestión.

A efectos de la aplicación del punto 6, las personas cuya identidad se desconozca podrán ser designadas por sus identificadores o su condición y los lugares o vehículos podrán ser designados con referencia a las personas objeto de la solicitud.

[…]»

36 En virtud del artículo L. 821-3, párrafo primero, del CSI:

«La solicitud se transmitirá al Presidente o, en su defecto, a uno de los miembros de la Comisión Nacional de Control de las Técnicas de Información mencionados en los puntos 2 y 3 del artículo L. 831-1, que enviará un dictamen al Primer Ministro en un plazo de veinticuatro horas. Si la solicitud es examinada por la composición restringida o por el pleno de la Comisión, se informará de ello sin demora al Primer Ministro y se emitirá un dictamen en un plazo de setenta y dos horas.»

37 El artículo L. 821-4 del CSI tiene el siguiente tenor:

«El Primer Ministro concederá la autorización de aplicación de las técnicas mencionadas en los capítulos I a IV del título V del presente libro por un máximo de cuatro meses. […] La autorización incluirá las motivaciones y las menciones previstas en los puntos 1 a 6 del artículo L. 821-2. La autorización será renovable en las mismas condiciones que las contempladas en el presente capítulo.

Cuando la autorización se conceda tras un dictamen desfavorable de la Comisión Nacional de Control de las Técnicas de Información, deberá indicar los motivos por los que no se ha seguido dicho dictamen.

[…]»

38 El artículo L. 833-4 del CSI, que figura en el capítulo III de dicho título, está redactado en los siguientes términos:

«Por iniciativa propia o cuando conozca de una reclamación presentada por toda persona que desee comprobar que no se le ha aplicado una técnica de información de manera ilegal, la Comisión efectuará el control de la técnica o técnicas invocadas para comprobar que han sido aplicadas en cumplimiento de lo dispuesto en el presente libro. La Comisión notificará al reclamante que se han efectuado las comprobaciones necesarias, sin confirmar ni desmentir su aplicación.»

39 El artículo L. 841-1, párrafos primero y segundo, del CSI tiene el siguiente tenor:

«Sin perjuicio de las disposiciones particulares previstas en el artículo L. 854-9 del presente Código, el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia) es competente para conocer, en las condiciones previstas en el capítulo III *bis* del título VII del libro VII del code de justice administrative (Código de Justicia Administrativa), de los recursos relativos a la aplicación de técnicas de información mencionadas en el título V del presente libro.

Podrán interponer recurso:

1.º Toda persona que desee comprobar que no se le ha aplicado una técnica de información de manera ilegal y que justifique la aplicación previa del procedimiento previo en el artículo L. 833-4.

2.º La Comisión Nacional de Control de las Técnicas de Información, en las condiciones previstas en el artículo L. 833-8.»

40 El título V del libro VIII de la parte legislativa del CSI, relativo a las «técnicas de recopilación de información sujetas a autorización», incluye, en particular, un capítulo 1, titulado «acceso administrativo a los datos de conexión», que contiene los artículos L. 851-1 a L. 851-7 del CSI.

41 El artículo L. 851-1 del CSI dispone que:

«En las condiciones establecidas en el capítulo I del título II del presente libro, podrá autorizarse recopilar de los operadores de comunicaciones electrónicas y de las personas mencionadas en el artículo L. 34-1 del [CPCE], así como de las personas indicadas en el artículo 6, punto I, apartados 1 y 2, de la loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Ley n.º 2004 -575 de 21 de junio de 2004, relativa a la Confianza en la Economía Digital) (JORF de 22 de junio de 2004, p. 11168), información o documentos tratados o conservados por sus redes o servicios de comunicaciones electrónicas, incluidos los datos técnicos relativos a la identificación de los números de abonado o de conexión a servicios de comunicaciones electrónicas, a la relación de todos los números de abonado o de conexión de una persona determinada, a la localización de los equipos terminales utilizados y a las comunicaciones de un abonado correspondientes a la relación de números de llamadas entrantes y salientes, la duración y la fecha de las comunicaciones.

No obstante lo dispuesto en el artículo L. 821-2, las solicitudes escritas y motivadas que tengan por objeto los datos técnicos relativos a la identificación de los números de abonado o de conexión a servicios de comunicaciones electrónicas, o la relación de todos los números de abonado o de conexión de una persona determinada, serán transmitidas directamente a la Comisión Nacional de Control de las Técnicas de Información por los agentes designados y autorizados individualmente de los servicios de información mencionados en los artículos L. 811-2 y L. 811-4. La Comisión emitirá su dictamen en las condiciones establecidas en el artículo L. 821-3.

Un servicio del Primer Ministro se encargará de recopilar las informaciones o documentos de los operadores y de las personas mencionadas en el párrafo primero del presente artículo. La Comisión Nacional de Control de las Técnicas de Información dispondrá de acceso permanente, completo, directo e inmediato a las informaciones o documentos recopilados.

Las normas de aplicación del presente artículo se establecerán mediante decreto consultado al Consejo de Estado, adoptado previo dictamen de la Commission nationale de l'informatique et des libertés (Comisión Nacional de Informática y Libertades, Francia) y de la Comisión Nacional de Control de las Técnicas de Información.»

42 A tenor de lo dispuesto en el artículo L. 851-2 del CSI:

«I. — En las condiciones establecidas en el capítulo I del título II del presente libro y únicamente con fines de prevención del terrorismo, podrá autorizarse individualmente la recopilación en tiempo real, en las redes de los operadores y de las personas mencionadas en el artículo L. 851-1, de las informaciones o documentos a que se refiere dicho artículo L. 851-1 relativos a una persona previamente identificada como sospechosa de estar relacionada con una amenaza. Cuando existan razones serias para considerar que una o varias personas pertenecientes al entorno de la persona respecto de la que se ha concedido la autorización pueden facilitar información en virtud de la finalidad que motiva la autorización, esta podrá concederse asimismo individualmente respecto de cada una de estas personas.

I *bis*. El Primer Ministro, previo dictamen de la Comisión Nacional de Control de las Técnicas de Información, establecerá el número máximo de autorizaciones concedidas con arreglo al presente artículo en vigor simultáneamente. Se notificarán a la Comisión la decisión por la que se fije dicho contingente y su distribución entre los ministros mencionados en el párrafo primero del artículo L. 821-2, así como el número de autorizaciones de interceptación concedidas.

[…]»

43 El artículo L. 851-3 del CSI prevé que:

«I. — En las condiciones establecidas en el capítulo I del título II del presente libro y únicamente con fines de prevención del terrorismo, podrá imponerse a los operadores y a las personas mencionadas en el artículo L. 851-1 aplicar en sus redes tratamientos automatizados de datos destinados, en función de los parámetros establecidos en la autorización, a detectar conexiones que pudieran suponer una amenaza terrorista.

Estos tratamientos automatizados utilizan exclusivamente las informaciones o documentos mencionados en el artículo L. 851-1, sin recopilar otros datos que los que responden a sus parámetros de diseño y sin permitir la identificación de las personas a las que se refieren las informaciones o documentos.

Dentro del respeto del principio de proporcionalidad, la autorización del Primer Ministro especificará el ámbito técnico de la aplicación de dichos tratamientos.

II. — La Comisión Nacional de Control de las Técnicas de Información emitirá un dictamen sobre la solicitud de autorización relativa a los tratamientos automatizados y los parámetros de detección establecidos. Esta dispondrá de acceso permanente, completo y directo a dichos tratamientos y a las informaciones o documentos recopilados. La Comisión será informada de cualquier modificación de los tratamientos y parámetros y podrá formular recomendaciones.

La primera autorización de aplicación de los tratamientos automatizados prevista en el apartado I del presente artículo se concederá por un período de dos meses. La autorización será renovable en las condiciones de duración establecidas en el capítulo I del título II del presente libro. La solicitud de renovación incluirá un historial del número de identificadores señalados por el tratamiento automatizado y un análisis de la pertinencia de dichos señalamientos.

III. — Las condiciones previstas en el artículo L. 871-6 se aplicarán a las operaciones materiales efectuadas con vistas a dicha aplicación por los operadores y las personas mencionadas en el artículo L. 851-1.

IV. — Cuando los tratamientos mencionados en el apartado I del presente artículo detecten datos susceptibles de caracterizar la existencia de una amenaza terrorista, el Primer Ministro o una de las personas en las que este haya delegado podrá autorizar, previo dictamen de la Comisión Nacional de Control de las Técnicas de Información emitido en las condiciones establecidas en el capítulo I del título II del presente libro, la identificación de la persona o de las personas afectadas y la recopilación de los datos correspondientes. Dichos datos se explotarán en un plazo de sesenta días a partir del momento de su recopilación y serán destruidos al término de dicho plazo, salvo en caso de que existan indicios serios que confirmen la existencia de una amenaza terrorista vinculada a una o varias de las personas afectadas.

[…]»

44 En virtud del artículo L. 851-4 del CSI:

«En las condiciones establecidas en el capítulo I del título II del presente libro, los datos técnicos relativos a la localización de los equipos terminales utilizados mencionados en el artículo L. 851-1 podrán ser recopilados a petición de la red y transmitidos en tiempo real por los operadores a un servicio del Primer Ministro.»

45 El artículo R. 851-5 del CSI, que figura en la parte reglamentaria de dicho Código, prevé que:

«I. — Las informaciones o documentos mencionados en el artículo L. 851-1 serán, con excepción del contenido de la correspondencia intercambiada o de la información consultada:

1.º Los enumerados en los artículos R. 10-13 y R. 10-14 del [CPCE] y en el artículo 1 del Decreto [n.º 2011-219].

2.º Los datos técnicos distintos de los mencionados en el punto 1:

a) que permiten localizar los equipos terminales;

b) relativos al acceso de los equipos terminales a las redes o a los servicios de comunicación al público en línea;

c) relativos a la conducción de las comunicaciones electrónicas a través de las redes;

d) relativos a la identificación y a la autentificación de un usuario, de una conexión, de una red o de un servicio de comunicación al público en línea;

e) relativos a las características de los equipos terminales y a los datos de configuración de sus soportes lógicos.

II. — Únicamente las informaciones y documentos mencionados en el punto 1 del apartado I podrán recopilarse con arreglo al artículo L. 851-1. Dicha recopilación tendrá lugar de forma diferida.

Las informaciones enumeradas en el punto 2 del apartado 1 únicamente podrán recopilarse con arreglo a los artículos L. 851-2 y L. 851-3 en las condiciones y dentro de los límites fijados en dichos artículos y sin perjuicio de la aplicación del artículo R. 851-9.»

CPCE

46 El artículo L. 34-1 del CPCE establece que:

«I. — El presente artículo se aplicará al tratamiento de datos personales en la prestación al público de servicios de comunicaciones electrónicas; en particular, se aplicará a las redes que acogen los dispositivos de recogida de datos y de identificación.

II. — Los operadores de comunicaciones electrónicas y, en particular, las personas cuya actividad consiste en ofrecer acceso a servicios de comunicación al público en línea, eliminarán o anonimizarán todos los datos de tráfico, sin perjuicio de lo estipulado en los apartados III, IV, V y VI.

Quienes presten al público servicios de comunicaciones electrónicas establecerán, en observancia de lo indicado en el párrafo anterior, procedimientos internos para atender las demandas de las autoridades competentes.

Quienes, en virtud de una actividad profesional principal o accesoria, ofrezcan al público una conexión que permita una comunicación en línea a través de un acceso a la red, incluso con carácter gratuito, estarán obligados al cumplimiento de las disposiciones aplicables a los operadores de comunicaciones electrónicas en virtud del presente artículo.

III. — A efectos de la investigación, la comprobación y la persecución de delitos o del incumplimiento de la obligación definida en el artículo L. 336-3 del code de la propriété intellectuelle (Código de la Propiedad Intelectual) o a efectos de la prevención de ataques a los sistemas de tratamiento automatizado de datos previstos y castigados por los artículos 323-1 a 323-3-1 del code pénal (Código Penal), y con el único objetivo de permitir, de ser necesario, la puesta a disposición de la autoridad judicial o de la alta autoridad mencionada en el artículo L. 331-12 del Código de la Propiedad Intelectual o de la autoridad nacional de seguridad de los sistemas de información mencionada en el artículo L. 2321-1 du code de la défense (Código de Defensa), podrán aplazarse durante un período máximo de un año las operaciones dirigidas a eliminar o a anonimizar determinadas categorías de datos técnicos. Mediante decreto consultado al Consejo de Estado, adoptado tras el dictamen de la Comisión Nacional de Informática y Libertades, se precisarán, en los límites marcados en el apartado VI, estas categorías de datos y la duración de su conservación, en función de la actividad de los operadores y de la naturaleza de las comunicaciones, así como las modalidades de indemnización, en su caso, de los sobrecostes identificables y específicos de las prestaciones garantizadas en tal concepto, a solicitud del Estado, por los operadores.

[…]

VI. — Los datos conservados y tratados en las condiciones fijadas en los apartados III, IV y V versarán exclusivamente sobre la identificación de los usuarios de los servicios suministrados por los operadores, sobre las características técnicas de las comunicaciones facilitadas por estos últimos y sobre la localización de los equipos terminales.

No podrán referirse en ningún caso al contenido de las correspondencias intercambiadas o a las informaciones consultadas, bajo cualquier forma, en el marco de esas comunicaciones.

La conservación y el tratamiento de los datos se realizará en el respeto de las disposiciones de la loi n.º 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Ley n.º 78-17 de 6 de enero de 1978, relativa a la Informática, a los Ficheros y a las Libertades).

Los operadores adoptarán todas las medidas para impedir una utilización de estos datos para otros fines distintos de los previstos en el presente artículo.»

47 El artículo R. 10-13 del CPCE está redactado en los siguientes términos:

«I. — Con arreglo al apartado III del artículo L. 34-1, los operadores de comunicaciones electrónicas conservarán, a los fines de la investigación, de la constatación y de la persecución de los delitos:

a) las informaciones que permitan identificar al usuario;

b) los datos relativos a los equipos terminales de comunicaciones utilizados;

c) las características técnicas, así como la fecha, hora y duración de cada comunicación;

d) los datos relativos a los servicios complementarios solicitados o utilizados y sus proveedores;

e) los datos que permitan identificar el o los destinatarios de la comunicación.

II. — En el caso de las actividades de telefonía, el operador conservará los datos mencionados en el apartado II y, además, los que permitan identificar el origen y la localización de la comunicación.

III. — Los datos mencionados en el presente artículo se conservarán durante un año desde el día de su registro.

IV. — Los sobrecostes identificables y específicos soportados por los operadores exigidos por las autoridades judiciales para el suministro de los datos comprendidos en las categorías mencionadas en el presente artículo se indemnizarán según las modalidades establecidas en el artículo R. 213-1 del code de procédure pénale (Código de Enjuiciamiento Criminal).»

48 El artículo R. 10-14 del CPCE prevé que:

«I. — Con arreglo al apartado IV del artículo L. 34-1, los operadores de comunicaciones electrónicas están autorizados a conservar, a los fines de sus operaciones de facturación y de pago, los datos de carácter técnico que permitan identificar al usuario, así como los mencionados en las letras b), c) y d) del apartado I del artículo R. 10-13.

II. — En el caso de las actividades de telefonía, los operadores podrán conservar, además de los datos mencionados en el apartado I, los datos de carácter técnico relativos a la localización de la comunicación, a la identificación del o de los destinatarios de la comunicación y los datos que permitan efectuar la facturación.

III. — Los datos mencionados en los apartados I y II del presente artículo solo podrán conservarse si son necesarios para la facturación y para el pago de los servicios prestados. Su conservación deberá limitarse al tiempo estrictamente necesario para este fin, que no podrá exceder de un año.

IV. — A efectos de la seguridad de las redes y de las instalaciones, los operadores podrán conservar durante un período que no podrá ser superior a tres meses:

a) los datos que permitan identificar el origen de la comunicación;

b) las características técnicas, así como la fecha, hora y duración de cada comunicación;

c) los datos de carácter técnico que permitan identificar el o los destinatarios de la comunicación;

d) los datos relativos a los servicios complementarios solicitados o utilizados y sus proveedores.»

Ley n.º 2004-575, de 21 de junio de 2004, relativa a la Confianza en la Economía Digital

49 El artículo 6 de la Ley n.º 2004-575, de 21 de junio de 2004, relativa a la Confianza en la Economía Digital (JORF de 22 de junio de 2004, p. 11168; en lo sucesivo, «LCEN») prevé que:

«I. — 1. Las personas cuya actividad consiste en ofrecer acceso a servicios de comunicación al público en línea informarán a sus abonados de la existencia de medios técnicos que permiten restringir el acceso a determinados servicios o seleccionarlos, y les propondrán, al menos, uno de estos medios.

[…]

2. Las personas físicas o jurídicas que almacenen, incluso con carácter gratuito, para la puesta a disposición del público mediante servicios de comunicación al público en línea, señales, textos, imágenes, sonidos o mensajes de cualquier naturaleza proporcionados por destinatarios de estos servicios no podrán incurrir en responsabilidad civil por las actividades o informaciones almacenadas a petición de un destinatario de estos servicios si no tenían efectivamente conocimiento de su carácter ilícito o de los hechos o circunstancias que revelan dicho carácter o si, desde el momento en que tuvieron conocimiento, actuaron sin demora para retirar estos datos o impedir el acceso a ellos.

[…]

II. — Las personas mencionadas en los puntos 1 y 2 del apartado I mantendrán y conservarán los datos de forma tal que permita la identificación de quien haya contribuido a la creación del contenido o de alguno de los contenidos de los servicios de los que son prestadores.

Estas podrán a disposición de quienes publiquen un servicio de comunicación al público en línea medios técnicos que les permitan cumplir los requisitos de identificación establecidos en el apartado III.

La autoridad judicial podrá requerir a los prestadores mencionados en los puntos 1 y 2 del apartado I que comuniquen los datos mencionados en el párrafo primero.

Las disposiciones de los artículos 226-17, 226-21 y 226-22 del Código Penal serán aplicables al tratamiento de estos datos.

Mediante decreto consultado al Consejo de Estado, adoptado tras el dictamen de la Comisión Nacional de Informática y Libertades, se definirán los datos mencionados en el párrafo primero y se determinarán la duración y las modalidades de su conservación.

[…]»

Decreto n.º 2011-219

50 El capítulo I del Decreto n.º 2011-219, adoptado sobre la base del artículo 6, apartado II, último párrafo, de la LCEN, contiene los artículos 1 a 4 de dicho Decreto.

51 El artículo 1 del Decreto n.º 2011-219 dispone que:

«Los datos mencionados en el apartado II del artículo 6 de la [LCEN], que las personas están obligadas a conservar en virtud de esta disposición, son los siguientes:

1.º Para las personas mencionadas en el punto 1 del apartado I de dicho artículo y para cada conexión de sus abonados:

a) el identificador de la conexión;

b) el identificador atribuido por estas personas al abonado;

c) el identificador de la terminal utilizada para la conexión cuando tienen acceso a la misma;

d) la fecha y hora del inicio y el fin de la conexión;

e) las características de la línea del abonado.

2.º Para las personas mencionadas en el punto 2 del apartado I de dicho artículo y para cada operación de creación:

a) el identificador de la conexión en el origen de la comunicación;

b) el identificador atribuido por el sistema de información al contenido objeto de la operación;

c) los tipos de protocolos utilizados para la conexión al servicio y para la transferencia de contenidos;

d) la naturaleza de la operación;

e) la fecha y la hora de la operación;

f) el identificador utilizado por el autor de la operación al llevarla a cabo.

3.º Para las personas mencionadas en los puntos 1 y 2 del apartado I de dicho artículo, las informaciones facilitadas por un usuario al suscribir un contrato o crear una cuenta:

a) el identificador de la conexión al crear la cuenta;

b) el nombre y apellidos o la razón social;

c) las direcciones postales asociadas;

d) los pseudónimos utilizados;

e) las direcciones de correo electrónico o de cuenta asociadas;

f) los números de teléfono;

g) la contraseña actualizada y los datos que permitan verificarla o modificarla.

4.º Para las personas mencionadas en los puntos 1 y 2 del apartado I de dicho artículo, cuando la suscripción del contrato o de la cuenta sea de pago, las informaciones siguientes relativas al pago, para cada operación de pago:

a) el tipo de pago utilizado;

b) la referencia del pago;

c) el importe;

d) la fecha y la hora de la transacción.

Los datos mencionados en los puntos 3 y 4 solo deben conservarse en la medida en que las personas los recopilan habitualmente.»

52 Con arreglo al artículo 2 de dicho Decreto:

«La contribución a una creación de contenido incluye las operaciones relativas a:

a) creaciones iniciales de contenidos;

b) modificaciones de los contenidos y de datos relacionados con los contenidos;

c) eliminación de contenidos.»

53 El artículo 3 de dicho Decreto prevé que:

«La duración de conservación de los datos mencionados en el artículo 1 será de un año:

a) por lo que se refiere a los datos mencionados en los puntos 1 y 2, a partir del día de la creación de los contenidos, para cada operación que contribuye a la creación de un contenido, tal como se define en el artículo 2;

b) por lo que se refiere a los datos mencionados en el punto 3, a partir del día de la rescisión del contrato o del cierre de la cuenta;

c) por lo que se refiere a los datos mencionados en el punto 4, a partir del día de emisión de la factura o de la operación de pago, para cada factura u operación de pago.»

Derecho belga

54 La Ley de 29 de mayo de 2016 modificó, en particular, la loi du 13 juin 2005 relative aux communications électroniques (Ley de 13 de junio de 2005 sobre Comunicaciones Electrónicas) (*Moniteur belge* de 20 de junio de 2005, p. 28070; en lo sucesivo, «Ley de 13 de junio de 2005»), el code d'instruction criminelle (Código de Enjuiciamiento Criminal) y la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Ley de 30 de noviembre de 1998 Orgánica de los Servicios de Inteligencia y Seguridad) (*Moniteur belge* de 18 de diciembre de 1998, p. 40312; en lo sucesivo, «Ley de 30 de noviembre de 1998»).

55 El artículo 126 de la Ley de 13 de junio de 2005, en su versión resultante de la Ley de 29 de mayo de 2016, dispone que:

«1. Sin perjuicio de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Ley de 8 de diciembre de 1992 sobre Protección de la Vida Privada con Respecto al Tratamiento de los Datos de Carácter Personal), los proveedores que presten al público servicios de telefonía, incluso a través de internet, de acceso a internet, de correo electrónico por internet, así como los operadores que proporcionen redes públicas de comunicación electrónica y los operadores que presten cualquiera de los servicios anteriores deberán conservar los datos indicados en el apartado 3 que generen o traten en el marco de la prestación de los servicios de comunicaciones de que se trate.

Este artículo no se refiere al contenido de las comunicaciones.

La obligación de conservar los datos contemplados en el apartado 3 se aplica igualmente a las llamadas fallidas, en la medida en que tales datos sean, en el marco de la prestación de los servicios de comunicación en cuestión:

1.º por lo que se refiere a los datos de la telefonía, generados o tratados por los operadores de servicios de comunicaciones electrónicas accesibles al público o de una red pública de comunicaciones electrónicas, o

2.º por lo que se refiere a los datos de internet, registrados por dichos proveedores.

2. Las autoridades enunciadas a continuación serán las únicas que, a su solicitud, podrán obtener de los proveedores y operadores indicados en el apartado 1, párrafo primero, los datos que se conserven con arreglo al presente artículo, para las finalidades y en las condiciones enumeradas a continuación:

1.º las autoridades judiciales, con fines de investigación, instrucción y persecución de delitos, a efectos de la ejecución de las medidas previstas en los artículos 46 *bis* y 88 *bis* del Código de Enjuiciamiento Criminal y en las condiciones previstas en los citados artículos;

2.º los servicios de inteligencia y seguridad, con el fin de cumplir misiones de inteligencia recurriendo a los métodos de recogida de datos previstos en los artículos 16/2, 18/7 y 18/8 de la Ley de 30 de noviembre de 1998 Orgánica de los Servicios de Inteligencia y Seguridad y en las condiciones establecidas en la presente ley;

3.º cualquier agente de la policía judicial del [Institut belge des services postaux et des télécommunications (Instituto belga de servicios postales y telecomunicaciones)], con fines de investigación, instrucción y persecución de delitos de los artículos 114 y 124 y del presente artículo;

4.º los servicios de emergencias que presten asistencia *in situ*, cuando, tras haber recibido una llamada de auxilio, no obtengan del proveedor o del operador en cuestión los datos de identificación de la persona que realizó la llamada mediante la base de datos a que se refiere el artículo 107, apartado 2, párrafo tercero, u obtengan datos incompletos o incorrectos. Solo podrán solicitarse los datos identificativos de la persona que realizó la llamada y, a más tardar, dentro de las 24 horas siguientes a su realización;

5.º cualquier agente de la policía judicial de la unidad de personas desaparecidas de la policía federal, en el marco de sus funciones de asistencia a personas en peligro, de búsqueda de personas cuya desaparición resulta sospechosa y cuando quepa presumir o existan indicios serios de que la integridad física de la persona desaparecida se encuentra en peligro inminente. Únicamente podrán

solicitarse al operador o al proveedor de que se trate, a través de un servicio de policía designado por el rey, los datos indicados en el apartado 3, párrafos primero y segundo, relativos a la persona desaparecida conservados durante las 48 horas anteriores a la solicitud de obtención de los datos;

6.º el Servicio de mediación para las telecomunicaciones, a efectos de identificar a la persona que haya hecho un uso indebido de una red o de un servicio de comunicaciones electrónicas, con arreglo a las condiciones mencionadas en el artículo 43 *bis*, apartado 3, punto 7, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (Ley de 21 de marzo de 1991 de Reforma de Determinadas Empresas Públicas). Solo podrán solicitarse los datos identificativos.

Los proveedores y operadores mencionados en el apartado 1, párrafo primero, dispondrán lo necesario para que los datos a que se refiere el apartado 3 sean accesibles sin límites desde Bélgica y para que tales datos y cualquier otra información necesaria relativa a ellos puedan transmitirse sin demora exclusivamente a las autoridades indicadas en este apartado.

Sin perjuicio de lo dispuesto en otras disposiciones legales, los proveedores y operadores a que se refiere el apartado 1, párrafo primero, no podrán utilizar los datos que conserven en cumplimiento de lo dispuesto en el apartado 3 para otros fines.

3. Los datos que permiten identificar al usuario o abonado y los medios de comunicación, a excepción de los datos específicamente previstos en los párrafos segundo y tercero, se conservarán durante los doce meses siguientes a la fecha en la que hubiera podido efectuarse por última vez una comunicación a través del servicio utilizado.

Los datos sobre acceso y conexión de los terminales a la red y al servicio, y de ubicación de esos equipos, incluido el punto de terminación de la red, se conservarán durante los doce meses siguientes a la fecha de la comunicación.

Los datos de comunicaciones, con exclusión de su contenido, incluidos los relativos a su origen y destino, se conservarán durante los doce meses siguientes a la fecha de la comunicación.

Mediante decreto adoptado por el Consejo de Ministros, a propuesta del Ministro de Justicia y del Ministro [competente en el ámbito de las comunicaciones electrónicas], y previo dictamen de la Comisión para la Protección de la Intimidad y del Instituto, el Rey establecerá los datos que han de conservarse por cada una de las categorías indicadas en los párrafos primero a tercero y los requisitos que esos datos deben reunir.

[…]»

Litigios principales y cuestiones prejudiciales

Asunto C-511/18

56 Mediante demandas presentadas los días 30 de noviembre de 2015 y 16 de marzo de 2016, que fueron acumuladas en el procedimiento principal, la Quadrature du Net, French Data Network y la Fédération des fournisseurs d'accès à Internet associatifs, así como Igwan.net, interpusieron ante el Conseil d'État (Consejo de Estado) un recurso que tenía por objeto la anulación de los Decretos n.ºs 2015-1185, 2015-1211, 2015-1639 y 2016-67, alegando, en particular, que dichos Decretos infringían la Constitución francesa, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en lo sucesivo, «CEDH») y las Directivas 2000/31 y 2002/58, en relación con los artículos 7, 8 y 47 de la Carta.

57 Por lo que se refiere, en particular, a los motivos basados en la infracción de la Directiva 2000/31, el órgano jurisdiccional remitente señala que las disposiciones del artículo L. 851-3 del CSI imponen a los operadores de comunicaciones electrónicas y a los prestadores de servicios técnicos la obligación de «aplicar en sus redes tratamientos automatizados de datos destinados, en función de los parámetros establecidos en la autorización, a detectar conexiones que pudieran suponer una amenaza terrorista». Esta técnica únicamente persigue recopilar, durante un tiempo limitado, de entre todos los datos de conexión tratados por esos operadores y prestadores, aquellos que pudieran estar relacionados con una infracción grave de ese tipo. En estas circunstancias, esas disposiciones, que no imponen una obligación general de supervisión activa, no infringen el artículo 15 de la Directiva 2000/31.

58 En lo que atañe a los motivos basados en la infracción de la Directiva 2002/58, el órgano jurisdiccional remitente considera que de las disposiciones de dicha Directiva, así como de la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, en lo sucesivo, «sentencia Tele2», EU:C:2016:970), resulta, en particular, que las disposiciones nacionales que imponen obligaciones a los proveedores de servicios de comunicaciones electrónicas, tales como la conservación generalizada e indiferenciada de los datos de tráfico y de localización de sus abonados y usuarios para los fines mencionados en el artículo 15, apartado 1, de dicha Directiva, entre los que figura la protección de la seguridad nacional, la defensa y la seguridad pública, están comprendidas en el ámbito de aplicación de la citada Directiva en la medida en que estas normativas regulan la actividad de tales proveedores. Lo mismo sucede con las normativas que regulan el acceso de las autoridades nacionales a los datos, así como su utilización.

59 El órgano jurisdiccional remitente deduce de ello que el ámbito de aplicación de la Directiva 2002/58 incluye tanto la obligación de conservación derivada del artículo L. 851-1 del CSI como el acceso administrativo a dichos datos, incluso en tiempo real, previsto en los artículos L. 851-1, L. 851-2 y L. 851-4 de dicho Código. Lo mismo ocurre, según este órgano jurisdiccional, con las disposiciones del artículo L. 851-3 de dicho Código que, si bien no imponen a los operadores en cuestión una obligación general de conservación, les exigen, sin embargo, aplicar en sus redes tratamientos automatizados destinados a detectar conexiones que pudieran suponer una amenaza terrorista.

60 En cambio, dicho órgano jurisdiccional considera que el ámbito de aplicación de la Directiva 2002/58 no incluye las disposiciones del CSI a que se refieren los recursos de anulación que versan sobre técnicas de recopilación de información que son aplicadas directamente por el Estado, pero no regulan las actividades de los proveedores de servicios de comunicaciones electrónicas imponiéndoles obligaciones específicas. Por tanto, no cabe considerar que esas disposiciones ejecutan el Derecho de la Unión y, en consecuencia, los motivos basados en que estas infringen la Directiva 2002/58 no pueden ser invocados eficazmente.

61 Así, para resolver los litigios relativos a la legalidad de los Decretos n.os 2015-1185, 2015-1211, 2015-1639 y 2016-67 a la luz de la Directiva 2002/58, en la medida en que fueron adoptados en desarrollo de los artículos L. 851-1 a L. 851-4 del CSI, se plantearían tres cuestiones de interpretación del Derecho de la Unión.

62 En lo tocante a la interpretación del artículo 15, apartado 1, de la Directiva 2002/58, el órgano jurisdiccional remitente se pregunta, en primer lugar, si la obligación de conservación generalizada e indiferenciada, impuesta a los proveedores de servicios de comunicaciones electrónicas sobre la base de los artículos L. 851-1 y R. 851-5 del CSI, debe considerarse, en especial a la luz de las garantías y controles que son inherentes al acceso administrativo a los datos de conexión y su utilización, como una injerencia justificada por el derecho a la seguridad garantizado en el artículo 6 de la Carta y las exigencias de la seguridad nacional, cuya responsabilidad incumbe únicamente a los Estados miembros en virtud del artículo 4 TUE.

63 En lo que atañe, en segundo lugar, a otras obligaciones que pueden imponerse a los proveedores de servicios de comunicaciones electrónicas, el órgano jurisdiccional remitente señala que las disposiciones del artículo L. 851-2 del CSI autorizan, únicamente con fines de prevención del terrorismo, a recopilar, de esas mismas personas, la información o los documentos que menciona el artículo L. 851-1 de dicho Código. Esta recopilación, referida únicamente a una o varias personas previamente identificadas como sospechosas de estar relacionadas con una amenaza terrorista, se efectúa en tiempo real. Lo mismo sucede con las disposiciones del artículo L. 851-4 del citado Código, que autorizan la transmisión en tiempo real por los operadores únicamente de los datos técnicos relativos a la localización de los equipos terminales. Estas técnicas se aplican para finalidades y en función de modalidades diferentes del acceso administrativo en tiempo real a los datos conservados con arreglo al CPCE y a la LCEN, sin, no obstante, imponer a los prestadores de que se trate una obligación de conservación suplementaria a la que se requiere para la facturación y prestación de sus servicios. De igual modo, las disposiciones del artículo L. 851-3 del CSI, que imponen a los proveedores de servicios la obligación de aplicar en sus redes un análisis automatizado de las conexiones, tampoco implican una conservación generalizada e indiferenciada.

64 Pues bien, por una parte, el órgano jurisdiccional remitente considera que tanto la conservación generalizada e indiferenciada como el acceso en tiempo real a los datos de conexión presentan, en un contexto caracterizado por amenazas graves y persistentes para la seguridad nacional, derivadas en particular del riesgo terrorista, una utilidad operativa sin parangón. En efecto, la conservación generalizada e indiferenciada permite a los servicios de información acceder a los datos relativos a las comunicaciones antes de que se hayan determinado los motivos para creer que la persona en cuestión representa una amenaza para la seguridad pública, la defensa o la seguridad del Estado. Además, el acceso en tiempo real a los datos de conexión permite seguir, con gran capacidad de respuesta, los comportamientos de personas susceptibles de representar una amenaza inmediata para el orden público.

65 Por otra parte, la técnica prevista en el artículo L. 851-3 del CSI permite detectar, sobre la base de criterios definidos con precisión a estos efectos, a las personas cuyos comportamientos, habida cuenta en especial de sus modalidades de comunicación, pueden suponer una amenaza terrorista.

66 En tercer lugar, en lo que atañe al acceso de las autoridades nacionales competentes a los datos conservados, el órgano jurisdiccional remitente se pregunta si la Directiva 2002/58, leída a la luz de la Carta, debe interpretarse en el sentido de que supedita en todos los casos la legalidad de los procedimientos de recopilación de datos de conexión a la obligación de informar a las personas afectadas, cuando tal información ya no pueda poner en peligro las investigaciones efectuadas por las autoridades competentes, o si cabe considerar que dichos procedimientos son legales habida cuenta de todas las demás garantías de procedimiento previstas por el Derecho nacional, siempre que estas últimas aseguren la tutela judicial efectiva.

67 En cuanto a las demás garantías de procedimiento, el órgano jurisdiccional remitente precisa, en particular, que toda persona que desee comprobar que no se le ha aplicado una técnica de información de manera ilegal puede dirigirse a la sección especializada del Conseil d'État (Consejo de Estado), que deberá comprobar, a la luz de los elementos que se le han comunicado fuera del procedimiento contradictorio, si el recurrente ha sido objeto de dicha técnica y si esta se ha aplicado respetando el libro VIII del CSI. Las facultades conferidas a dicha sección para instruir los recursos garantizan la efectividad del control judicial que ejerce. De este modo, es competente para instruir los recursos, apreciar de oficio todas las ilegalidades que detecte y ordenar a la Administración la adopción de todas las medidas útiles para subsanar las ilegalidades constatadas. Por otra parte, corresponde a la Comisión Nacional de Control de las Técnicas de Información comprobar que las técnicas de recopilación de información han sido aplicadas, en el territorio nacional, conforme a las exigencias previstas en el CSI. De este modo, la circunstancia de que las disposiciones legislativas controvertidas

en el litigio principal no prevean que las personas afectadas sean notificadas de las medidas de vigilancia de las que han sido objeto no constituye, por sí sola, una vulneración excesiva al derecho al respeto de la vida privada.

68 En estas circunstancias, el Conseil d'État (Consejo de Estado) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Debe considerarse la obligación de conservación generalizada e indiferenciada, impuesta a los prestadores de servicios al amparo de las disposiciones habilitantes del artículo 15, apartado 1, de la Directiva [2002/58], en un contexto caracterizado por amenazas graves y persistentes para la seguridad nacional, en particular por el riesgo terrorista, una injerencia justificada por el derecho a la seguridad reconocido en el artículo 6 de la [Carta] y las exigencias de la seguridad nacional, cuya responsabilidad incumbe únicamente a los Estados miembros en virtud del artículo 4 [TUE]?

2) ¿Debe interpretarse la Directiva [2002/58], a la luz de la [Carta], en el sentido de que permite medidas legislativas, tales como las medidas de recopilación en tiempo real de datos de tráfico y localización de personas concretas, que, si bien afectan a los derechos y obligaciones de los proveedores de servicios de comunicaciones electrónicas, no les imponen sin embargo una obligación específica de conservación de sus datos?

3) ¿Debe interpretarse la Directiva [2002/58], a la luz de la [Carta], en el sentido de que supedita en todos los casos la legalidad de los procedimientos de recopilación de los datos de conexión a la obligación de informar a las personas afectadas, cuando tal información ya no pueda poner en peligro las investigaciones efectuadas por las autoridades competentes, o cabe considerar que dichos procedimientos son legales habida cuenta de todas las demás garantías de procedimiento existentes, siempre que estas últimas aseguren la efectividad del derecho a recurrir?»

Asunto C-512/18

69 Mediante demanda presentada el 1 de septiembre de 2015, French Data Network, la Quadrature du Net y la Fédération des fournisseurs d'accès à Internet associatifs interpusieron ante el Conseil d'État (Consejo de Estado) un recurso que tenía por objeto la anulación de la decisión denegatoria presunta, derivada del silencio del Primer Ministro, respecto a su solicitud de derogación del artículo R. 10-13 del CPCE y del Decreto n.º 2011-219, alegando, en particular, que dichas normas infringen el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 de la Carta. Se admitió la intervención en el procedimiento principal de Privacy International y Center for Democracy and Technology.

70 Por lo que se refiere al artículo R. 10-13 del CPCE y a la obligación de conservación generalizada e indiferenciada de los datos relativos a las comunicaciones que este establece, el órgano jurisdiccional remitente, que formula consideraciones similares a las manifestadas en el marco del asunto C-511/18, observa que dicha conservación permite a la autoridad judicial acceder a los datos de las comunicaciones efectuadas por una persona antes de que haya sido identificada como sospechosa de haber cometido un delito, por lo que presenta una utilidad operativa sin parangón para la investigación, descubrimiento y persecución de delitos.

71 En cuanto al Decreto n.º 2011-219, el órgano jurisdiccional remitente considera que el artículo 6, apartado II, de la LCEN, que impone una obligación de mantenimiento y de conservación únicamente de los datos relativos a la creación de contenido, no está comprendido en el ámbito de aplicación de la Directiva 2002/58, en la medida en que este se limita, con arreglo a su artículo 3, apartado 1, a la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Unión, sino en el ámbito de aplicación de la Directiva 2000/31.

72 Este órgano jurisdiccional considera, no obstante, que del artículo 15, apartados 1 y 2, de la Directiva 2000/31 se desprende que esta no establece una prohibición de principio de conservar los datos relativos a la creación de contenido, a la que únicamente cabría establecer excepciones. De este modo, se plantea la cuestión de si los artículos 12, 14 y 15 de dicha Directiva, en relación con los artículos 6 a 8 y 11 y 52, apartado 1, de la Carta, deben interpretarse en el sentido de que permiten a un Estado miembro adoptar una normativa nacional, como el artículo 6, apartado II, de la LCEN, que impone a las personas afectadas la obligación de conservar los datos que puedan permitir la identificación de quien haya contribuido a la creación del contenido o de alguno de los contenidos de los servicios que aquellas prestan, con el fin de que la autoridad judicial pueda requerir, en su caso, la comunicación de los mismos para que se respeten las normas en materia de responsabilidad civil o penal.

73 En estas circunstancias, el Conseil d'État (Consejo de Estado) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Debe considerarse la obligación de conservación generalizada e indiferenciada, impuesta a los proveedores de servicios sobre la base de las disposiciones habilitantes del artículo 15, apartado 1, de la Directiva [2002/58], en particular a la vista de las garantías y de los controles que acompañan posteriormente la recogida y la utilización de estos datos de conexión, una injerencia justificada por el derecho a la seguridad garantizado en el artículo 6 de la [Carta] y las exigencias de la seguridad nacional, cuya responsabilidad incumbe únicamente a los Estados miembros en virtud del artículo 4 [TUE]?

2) ¿Deben interpretarse las disposiciones de la Directiva [2000/31], a la luz de los artículos 6, 7, 8 y 11, así como 52, apartado 1, de la [Carta], en el sentido de que permiten a un Estado miembro establecer una normativa nacional que obligue a las personas cuya actividad consista en ofrecer acceso a servicios de comunicación al público en línea y a las personas físicas o jurídicas que almacenen, incluso con carácter gratuito, para la puesta a disposición del público mediante servicios de comunicación al público en línea, señales, textos, imágenes, sonidos o mensajes de cualquier naturaleza proporcionados por destinatarios de estos servicios, a conservar los datos que puedan permitir la identificación de quien haya contribuido a la creación del contenido o de alguno de los contenidos de los servicios que aquellas prestan, con el fin de que la autoridad judicial pueda requerir, en su caso, la comunicación de los mismos para que se respeten las normas en materia de responsabilidad civil o penal?»

Asunto C-520/18

74 Mediante demandas presentadas los días 10, 16, 17 y 18 de enero de 2017, que fueron acumuladas en el marco del procedimiento principal, el Ordre des barreaux francophones et germanophone, la Académie Fiscale ASBL y UA, la Liga voor Mensenrechten ASBL y la Ligue des Droits de l'Homme ASBL, así como VZ, WY y XX, interpusieron ante la Cour constitutionnelle (Tribunal Constitucional, Bélgica) un recurso que tenía por objeto la anulación de la Ley de 29 de mayo de 2016, basándose en que esta infringe los artículos 10 y 11 de la Constitución belga, puestos en relación con los artículos 5, 6 a 11, 14, 15, 17 y 18 del CEDH, los artículos 7, 8, 11 y 47, así como el artículo 52, apartado 1, de la Carta, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966 y que entró en vigor el 23 de marzo de 1976, los principios generales de seguridad jurídica, de proporcionalidad y de autodeterminación en materia de información y el artículo 5 TUE, apartado 4.

75 En apoyo de sus recursos, los recurrentes en el litigio principal alegan, en esencia, que la ilegalidad de la Ley de 29 de mayo de 2016 tiene su origen, en particular, en el hecho de que esta excede de lo estrictamente necesario y no establece garantías de protección suficientes. Concretamente, ni sus disposiciones relativas a la conservación de los datos ni las que regulan el acceso de las autoridades a los datos conservados cumplen las exigencias que se derivan de la sentencia de 8 de abril de 2014,

Digital Rights Ireland y otros (C-293/12 y C-594/12, en lo sucesivo, «sentencia Digital Rights», EU:C:2014:238), y de la sentencia de 21 de diciembre de 2016, Tele2 (C-203/15 y C-698/15, EU:C:2016:970). En su opinión, dichas disposiciones conllevan el riesgo de que se establezcan perfiles de personalidad, con los abusos que pueden derivarse de ello por parte de las autoridades competentes, y no prevén un nivel adecuado de seguridad y de protección de los datos conservados. Por último, esta Ley se aplica a personas que están sujetas a secreto profesional y a personas sobre las que recae una obligación de confidencialidad, y se refiere a datos de comunicación personales de carácter sensible, sin incluir garantías especiales que protejan estos últimos datos.

76 El órgano jurisdiccional remitente indica que los datos que deben conservar los proveedores de servicios de telefonía, incluso a través de internet, de acceso a internet, de correo electrónico por internet, así como los operadores que proporcionen redes públicas de comunicación electrónica, con arreglo a la Ley de 29 de mayo de 2016, son idénticos a los enumerados en 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 (DO 2006, L 105, p. 54), sin que se establezca una distinción por lo que se refiere a las personas afectadas o en función del objetivo perseguido. En relación con este último aspecto, dicho órgano jurisdiccional precisa que el objetivo perseguido por el legislador a través de esta Ley no solo es luchar contra el terrorismo y la pornografía infantil, sino también poder utilizar los datos conservados en una gran variedad de situaciones en el marco de la investigación penal. Además, el órgano jurisdiccional remitente declara que de la exposición de motivos de dicha Ley se desprende que el legislador nacional consideró que era imposible, a la luz del objetivo perseguido, establecer una obligación de conservación selectiva y diferenciada, y que optó por acompañar la obligación de conservación general e indiferenciada de garantías estrictas, tanto desde el punto de vista de los datos conservados como desde el punto de vista del acceso a los mismos, a fin de reducir al mínimo la injerencia en el derecho al respeto de la vida privada.

77 El órgano jurisdiccional remitente añade que el artículo 126, apartado 2, puntos 1 y 2, de la Ley de 13 de junio de 2005, en su versión resultante de la Ley de 29 de mayo de 2016, establece las condiciones en las que, respectivamente, las autoridades judiciales y los servicios de inteligencia y de seguridad pueden acceder a los datos conservados, de tal modo que el examen de la legalidad de dicha Ley a la luz de las exigencias del Derecho de la Unión debe suspenderse hasta que el Tribunal de Justicia se pronuncie en dos procedimientos prejudiciales, pendientes ante él, relativos a dicho acceso.

78 Por último, el órgano jurisdiccional remitente afirma que la Ley de 29 de mayo de 2016 tiene por objeto permitir una instrucción penal eficaz y sanciones efectivas en caso de abusos sexuales a menores, así como facilitar la identificación del autor de dicho delito, también cuando haga uso de medios de comunicaciones electrónicas. En el procedimiento seguido ante él, se prestó especial atención a este respecto a las obligaciones positivas que se desprenden de los artículos 3 y 8 del CEDH. Estas obligaciones pueden resultar asimismo de las disposiciones correspondientes de la Carta, que pueden incidir en la interpretación del artículo 15, apartado 1, de la Directiva 2002/58.

79 En estas circunstancias, la Cour Constitutionnelle (Tribunal Constitucional) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Debe interpretarse el artículo 15, apartado 1, de la Directiva [2002/58], en relación con el derecho a la seguridad, consagrado en el artículo 6 de la [Carta], y el derecho al respeto de los datos personales, garantizado por los artículos 7, 8 y 52, apartado 1, de la [Carta], en el sentido de que se opone a una normativa nacional, como la controvertida, que impone a los operadores y proveedores de servicios de comunicaciones electrónicas la obligación general de conservar los datos de tráfico y de localización, en el sentido de la Directiva [2002/58], que generan o someten a tratamiento en el marco de la prestación de esos servicios, y cuyo objetivo no es únicamente la

investigación, descubrimiento y persecución de delitos graves, sino también la seguridad nacional, la defensa del territorio, la seguridad pública, la investigación, descubrimiento y persecución de delitos no graves o la prevención de la utilización no autorizada del sistema de comunicaciones electrónicas, o la consecución de otro objetivo previsto en el artículo 23, apartado 1, del Reglamento [2016/679] y que, además, está sujeta a garantías reguladas de forma precisa en dicha normativa atinentes a la conservación de los datos y al acceso a ellos?

2) ¿Debe interpretarse el artículo 15, apartado 1, de la Directiva [2002/58], en relación con los artículos 4, 7, 8, 11 y 52, apartado 1, de la [Carta], en el sentido de que se opone a una normativa nacional, como la controvertida, que impone a los operadores y proveedores de servicios de comunicaciones electrónicas la obligación general de conservar los datos de tráfico y de localización, en el sentido de la Directiva [2002/58], que generan o someten a tratamiento en el marco de la prestación de esos servicios, cuando dicha normativa tiene fundamentalmente por objeto cumplir las obligaciones positivas que incumben a la autoridad en virtud de los artículos 4 y [7] de la Carta, consistentes en establecer un marco jurídico que permita que se investiguen y sancionen en el ámbito penal de forma efectiva los abusos sexuales a menores y se identifique al autor de esos delitos, también cuando haga uso de medios de comunicación electrónicos?

3) Si, sobre la base de las respuestas a las cuestiones prejudiciales primera y segunda, la Cour constitutionnelle llegase a la conclusión de que la Ley impugnada infringe una o varias de las obligaciones que se derivan de las disposiciones mencionadas en dichas cuestiones, ¿podría mantener con carácter provisional los efectos de la Ley de [29 de mayo de 2016] para evitar la inseguridad jurídica y permitir que los datos recabados y conservados con anterioridad puedan seguir utilizándose para los fines previstos en la Ley?»

Sobre el procedimiento ante el Tribunal de Justicia

80 Mediante auto del Presidente del Tribunal de 25 de septiembre de 2018 se ordenó acumular los asuntos C-511/18 y C-512/18 a efectos de las fases escrita y oral y de la sentencia. Mediante auto del Presidente del Tribunal de Justicia de 9 de julio de 2020 se ordenó acumular a los citados asuntos el asunto C-520/18 a efectos de la sentencia.

Sobre las cuestiones prejudiciales

Primeras cuestiones prejudiciales planteadas en los asuntos C-511/18 y C-512/18 y sobre las cuestiones prejudiciales primera y segunda planteadas en el asunto C-520/18

81 Mediante las primeras cuestiones prejudiciales planteadas en los asuntos C-511/18 y C-512/18 y mediante las cuestiones prejudiciales primera y segunda planteadas en el asunto C-520/18, que procede examinar conjuntamente, los órganos jurisdiccionales remitentes solicitan, en esencia, que se dilucide si el artículo 15, apartado 1, de la Directiva 2002/58 debe interpretarse en el sentido de que se opone a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas, para los fines contemplados en dicho artículo 15, apartado 1, una obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización.

Observaciones preliminares

82 De los autos aportados al Tribunal de Justicia se desprende que las normativas controvertidas en los litigios principales cubren la totalidad de los medios de comunicaciones electrónicas y se aplican a la totalidad de los usuarios de estos medios, sin que se establezca ninguna diferenciación o excepción a este respecto. Además, los datos que estas normativas exigen conservar a los proveedores de servicios

de comunicaciones electrónicas son, en particular, los necesarios para rastrear el origen de una comunicación y su destino, determinar la fecha, hora, duración y tipo de la comunicación, identificar el material de comunicación utilizado y localizar los equipos terminales y las comunicaciones, datos entre los que figuran, en particular, el nombre y la dirección del abonado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet. En cambio, dichos datos no cubren el contenido de las comunicaciones de que se trate.

83 De este modo, los datos que, con arreglo a las normativas nacionales controvertidas en los litigios principales, deben conservarse durante un año permiten, en particular, saber quién es la persona con la que se ha comunicado el usuario de un medio de comunicación electrónico y por qué medio se ha producido dicha comunicación, determinar la fecha, hora y duración de las comunicaciones y de las conexiones a Internet, así como el lugar desde el que estas se han producido, y conocer la localización de los equipos terminales sin que se transmita necesariamente la comunicación. Además, dichos datos ofrecen la posibilidad de determinar la frecuencia de las comunicaciones del usuario con ciertas personas durante un período determinado. Por último, por lo que se refiere a la normativa nacional controvertida en los asuntos C-511/18 y C-512/18, parece que esta, en la medida en que cubre asimismo los datos relativos a la conducción de las comunicaciones electrónicas por las redes, permite asimismo identificar la naturaleza de la información consultada en línea.

84 En cuanto a las finalidades que se persiguen, procede señalar que las normativas controvertidas en los asuntos C-511/18 y C-512/18 persiguen, entre otras finalidades, la investigación, la comprobación y la persecución de delitos en general, la independencia nacional, la integridad del territorio y la defensa nacional, los principales intereses de la política exterior, la ejecución de los compromisos adquiridos por Francia a nivel europeo e internacional, los principales intereses económicos, industriales y científicos de Francia, así como la prevención del terrorismo, de los atentados contra la forma republicana de las instituciones y de los actos de violencia colectiva que puedan alterar gravemente el orden público. En lo que atañe a la normativa controvertida en el asunto C-520/18, esta tiene como objetivos, entre otros, la investigación, el descubrimiento y la persecución de delitos, así como la salvaguarda de la seguridad nacional, de la defensa del territorio y de la seguridad pública.

85 Los órganos jurisdiccionales remitentes se preguntan, en particular, sobre las posibles repercusiones del derecho a la seguridad consagrado en el artículo 6 de la Carta en la interpretación del artículo 15, apartado 1, de la Directiva 2002/58. De igual modo, se preguntan si la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que supone la conservación de los datos prevista en las normativas controvertidas en los litigios principales puede, atendiendo a la existencia de normas que restringen el acceso de las autoridades nacionales a los datos conservados, considerarse justificada. Por otra parte, puesto que, según el Conseil d'État (Consejo de Estado), dicha cuestión se plantea en un contexto caracterizado por amenazas graves y persistentes para la seguridad nacional, debe apreciarse asimismo a la luz del artículo 4 TUE, apartado 2. La Cour constitutionnelle (Tribunal Constitucional), por su parte, subraya que la normativa nacional controvertida en el asunto C-520/18 también aplica obligaciones positivas resultantes de los artículos 4 y 7 de la Carta, que consisten en establecer un marco jurídico que permita sancionar de forma efectiva los abusos sexuales a menores.

86 Aunque tanto el Conseil d'État (Consejo de Estado) como la Cour constitutionnelle (Tribunal Constitucional) parten de la premisa de que las normativas nacionales controvertidas en los litigios principales, que regulan la conservación de los datos de tráfico y de localización, así como el acceso a estos datos por parte de las autoridades nacionales para los fines previstos en el artículo 15, apartado 1, de la Directiva 2002/58, tales como la protección de la seguridad nacional, están comprendidas en el ámbito de aplicación de dicha Directiva, algunas partes de los litigios principales y algunos de los Estados miembros que han presentado observaciones escritas ante el Tribunal de Justicia disienten a este respecto, en particular por lo que se refiere a la interpretación del artículo 1, apartado 3, de dicha Directiva. Por lo tanto, procede examinar antes de nada si estas normativas están comprendidas en el ámbito de aplicación de dicha Directiva.

Sobre el ámbito de aplicación de la Directiva 2002/58

87 La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International y el Center for Democracy and Technology alegan, en esencia, basándose a este respecto en la jurisprudencia del Tribunal de Justicia relativa al ámbito de aplicación de la Directiva 2002/58, que tanto la conservación de los datos como el acceso a los datos conservados están comprendidos en este ámbito de aplicación, con independencia de que dicho acceso tenga lugar en tiempo diferido o en tiempo real. Consideran que, dado que el objetivo de protección de la seguridad nacional se menciona expresamente en el artículo 15, apartado 1, de la citada Directiva, la consecución de este objetivo no supone que esta no sea aplicable. El artículo 4 TUE, apartado 2, al que se refieren los órganos jurisdiccionales remitentes, no afecta, en su opinión, a esta apreciación.

88 En lo tocante a las medidas de recopilación de información que las autoridades francesas competentes aplican directamente sin regular la actividad de los proveedores de servicios de comunicaciones electrónicas imponiéndoles obligaciones específicas, el Center for Democracy and Technology observa que estas medidas están comprendidas necesariamente en el ámbito de aplicación de la Directiva 2002/58 y en el de la Carta, puesto que constituyen excepciones al principio de confidencialidad garantizado en el artículo 5 de dicha Directiva. En consecuencia, estas medidas deben respetar los requisitos derivados de su artículo 15, apartado 1.

89 En cambio, los Gobiernos francés, checo y estonio, Irlanda, los Gobiernos chipriota, húngaro, polaco, sueco y del Reino Unido aducen, en esencia, que la Directiva 2002/58 no se aplica a normativas nacionales como las controvertidas en los litigios principales, porque estas normativas tienen como finalidad la protección de la seguridad nacional. Las actividades de los servicios de inteligencia, en la medida en que pretenden mantener el orden público y salvaguardar la seguridad interior y la integridad territorial, son funciones esenciales de los Estados miembros y, en consecuencia, son competencia exclusiva de estos, como pone de manifiesto, en particular, el artículo 4 TUE, apartado 2, tercera frase.

90 Estos Gobiernos e Irlanda se refieren además al artículo 1, apartado 3, de la Directiva 2002/58, que, a su parecer, excluye del ámbito de aplicación de la misma, a semejanza de lo que ya preveía el artículo 3, apartado 2, primer guion, de la Directiva 95/46, las actividades que tengan por objeto la seguridad pública, la defensa y la seguridad del Estado. Se basan, a este respecto, en la interpretación de esta última disposición que figura en la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión (C-317/04 y C-318/04, EU:C:2006:346).

91 A este respecto, procede indicar que, con arreglo a su artículo 1, apartado 1, la Directiva 2002/58 establece, en particular, la armonización de las disposiciones nacionales necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas.

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

93 Además, el artículo 3 de la Directiva 2002/58 dispone que dicha Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Unión, incluidas las redes públicas de

comunicaciones que den soporte a dispositivos de identificación y recopilación de datos (en lo sucesivo, «servicios de comunicaciones electrónicas»). Por lo tanto, debe considerarse que dicha Directiva regula las actividades de los proveedores de tales servicios (sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 33 y jurisprudencia citada).

94 En este marco, el artículo 15, apartado 1, de la Directiva 2002/58 autoriza a los Estados miembros a adoptar, cumpliendo los requisitos que prescribe, «medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de [esta] Directiva» (sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 71).

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

96 Basándose principalmente en estas consideraciones, el Tribunal de Justicia ha declarado que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con su artículo 3, debe interpretarse en el sentido de que están incluidas en el ámbito de aplicación de esta Directiva no solo una medida legislativa que obliga a los proveedores de servicios de comunicaciones electrónicas a conservar los datos de tráfico y de localización, sino también una medida legislativa que les obliga a permitir a las autoridades nacionales competentes el acceso a estos datos. En efecto, tales medidas legislativas implican necesariamente un tratamiento de los datos por esos proveedores y, en la medida en que regulan las actividades de dichos proveedores, no pueden asimilarse a actividades propias de los Estados, mencionadas en el artículo 1, apartado 3, de dicha Directiva (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartados 35 y 37 y jurisprudencia citada).

97 Además, habida cuenta de las consideraciones que figuran en el apartado 95 de la presente sentencia y del sistema general de la Directiva 2002/58, una interpretación de esta Directiva según la cual las medidas legales contempladas en su artículo 15, apartado 1, están excluidas del ámbito de aplicación de dicha Directiva, debido a que las finalidades a las que deben responder esas medidas coinciden sustancialmente con las finalidades que persiguen las actividades mencionadas en el artículo 1, apartado 3, de la misma Directiva, privaría a dicho artículo 15, apartado 1, de toda eficacia (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 72 y 73).

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

99 Las disposiciones del artículo 4 TUE, apartado 2, a las que se han referido los Gobiernos mencionados en el apartado 89 de la presente sentencia, no pueden desvirtuar esta conclusión. En efecto, según reiterada jurisprudencia del Tribunal de Justicia, si bien corresponde a los Estados miembros determinar sus intereses esenciales de seguridad y adoptar las medidas adecuadas para garantizar su seguridad interior y exterior, el mero hecho de que se haya adoptado una medida nacional con el fin de proteger la seguridad nacional no puede dar lugar a la inaplicabilidad del Derecho de la Unión ni dispensar a los Estados miembros de la necesaria observancia de dicho Derecho [véanse, en este sentido, las sentencias de 4 de junio de 2013, ZZ, C-300/11, EU:C:2013:363, apartado 38; de

20 de marzo de 2018, Comisión/Austria (Imprenta del Estado), C-187/16, EU:C:2018:194, apartados 75 y 76, y de 2 de abril de 2020, Comisión/Polonia, Hungría y República Checa (Mecanismo temporal de reubicación de solicitantes de protección internacional), C-715/17, C-718/17 y C-719/17, EU:C:2020:257, apartados 143 y 170].

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

101 Sin embargo, en vista de las consideraciones expuestas en los apartados 93, 95 y 96 de la presente sentencia, esta jurisprudencia no puede aplicarse a la interpretación del artículo 1, apartado 3, de la Directiva 2002/58. En efecto, como ha señalado, en esencia, el Abogado General en los puntos 70 a 72 de sus conclusiones presentadas en los asuntos acumulados La Quadrature du Net y otros (C-511/18 y C-512/18, EU:C:2020:6), el artículo 3, apartado 2, primer guion, de la Directiva 95/46, al que se refiere dicha jurisprudencia, excluía del ámbito de aplicación de esta última Directiva, de manera general, el «tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado», sin distinguir en función del autor del tratamiento de datos. En cambio, en la interpretación del artículo 1, apartado 3, de la Directiva 2002/58, esta distinción resulta necesaria. En efecto, como se desprende de los apartados 94 a 97 de la presente sentencia, el conjunto de tratamientos de datos personales efectuados por los proveedores de servicios de comunicaciones electrónicas está comprendido en el ámbito de aplicación de dicha Directiva, incluidos los tratamientos que se derivan de las obligaciones que les imponen los poderes públicos, mientras que estos últimos tratamientos podían, en su caso, estar comprendidos en el ámbito de aplicación de la excepción prevista en el artículo 3, apartado 2, primer guion, de la Directiva 95/46, dada la formulación más amplia de dicha disposición, referida a todos los tratamientos de datos personales que tengan por objeto la seguridad pública, la defensa o la seguridad del Estado, con independencia de quién sea su autor.

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

103 En cambio, cuando los Estados miembros aplican directamente medidas que suponen excepciones a la confidencialidad de las comunicaciones electrónicas, sin imponer obligaciones de tratamiento a los proveedores de servicios de tales comunicaciones, la protección de los datos de las personas afectadas no está regulada por la Directiva 2002/58, sino únicamente por el Derecho nacional, sin perjuicio de la aplicación de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de

dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89), de modo que las medidas en cuestión deben cumplir en particular la legislación nacional de rango constitucional y los requisitos del CEDH.

104 De las consideraciones anteriores se desprende que una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar los datos de tráfico y de localización a efectos de la protección de la seguridad nacional y de la lucha contra la delincuencia, como las controvertidas en los litigios principales, está comprendida en el ámbito de aplicación de la Directiva 2002/58.

Sobre la interpretación del artículo 15, apartado 1, de la Directiva 2002/58

105 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 (véase, en este sentido, la sentencia de 17 de abril de 2018, Egenberger, C-414/16, EU:C:2018:257, apartado 44).

106 La Directiva 2002/58 tiene como objetivo, como se desprende en particular de sus considerandos 6 y 7, proteger a los usuarios de los servicios de comunicaciones electrónicas frente a los riesgos que suponen para sus datos personales y su intimidad las nuevas tecnologías y, en especial, la creciente capacidad de almacenamiento y tratamiento informático de datos. En particular, dicha Directiva pretende, como indica su considerando 2, garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de la Carta. A este respecto, de la exposición de motivos de la propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas [COM(2000) 385 final], que dio lugar a la Directiva 2002/58, se desprende que el legislador de la Unión pretendió que «[siguiera] estando garantizado un nivel elevado de protección de los datos personales y la intimidad para todos los servicios de comunicaciones electrónicas con independencia de la tecnología utilizada».

107 A tal efecto, 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.

108 Por lo que se refiere, en particular, al tratamiento y al almacenamiento de los datos de tráfico por parte de los proveedores de servicios de comunicaciones electrónicas, del artículo 6 y de los considerandos 22 y 26 de la Directiva 2002/58 se desprende que este tratamiento solo está autorizado en la medida y durante el tiempo necesarios para la comercialización de los servicios, la facturación de estos y la prestación de servicios con valor añadido. Una vez expirado este plazo, los datos que hayan sido tratados y almacenados deberán eliminarse o hacerse anónimos. En relación con los datos de localización distintos de los datos de tráfico, el artículo 9, apartado 1, de dicha Directiva establece que esos datos solo podrán tratarse conforme a ciertos requisitos y tras haberse hecho anónimos o previo consentimiento de los usuarios o abonados (sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 86 y jurisprudencia citada).

109 Así pues, al adoptar esta Directiva, el legislador de la Unión concretó los derechos consagrados en los artículos 7 y 8 de la Carta, de modo que los usuarios de los medios de comunicaciones electrónicas tienen derecho a contar con que, en principio, de no mediar su consentimiento, sus comunicaciones y los datos relativos a ellas permanezcan anónimos y no puedan registrarse.

110 Sin embargo, el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros establecer excepciones a la obligación de principio, enunciada en el artículo 5, apartado 1, de dicha Directiva, de garantizar la confidencialidad de los datos personales y a las obligaciones correspondientes, mencionadas en particular en los artículos 6 y 9 de dicha Directiva, cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional, la defensa, la seguridad pública, o para la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por uno de esos motivos.

111 Dicho esto, la facultad de establecer excepciones a los derechos y obligaciones previstos en los artículos 5, 6 y 9 de la Directiva 2002/58 no puede justificar que la excepción a la obligación de principio de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos relativos a ellas y, en particular, a la prohibición de almacenar esos datos, establecida expresamente en el artículo 5 de dicha Directiva, se convierta en la regla (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 89 y 104).

112 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 legislativa que se adopte en virtud de esta disposición ha de responder efectiva y estrictamente a uno de ellos (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 52 y jurisprudencia citada).

113 Además, del artículo 15, apartado 1, tercera frase, de la Directiva 2002/58 se desprende que los Estados miembros solo pueden adoptar medidas legales para limitar el alcance de los derechos y obligaciones contemplados en los artículos 5, 6 y 9 de dicha Directiva que sean conformes con los principios generales del Derecho de la Unión, entre los que figura el principio de proporcionalidad, y con los derechos fundamentales garantizados por la Carta. A este respecto, el Tribunal de Justicia ya ha declarado que la obligación impuesta por un Estado miembro a los proveedores de servicios de comunicaciones electrónicas, mediante una normativa nacional, de conservar los datos de tráfico con el fin de hacerlos accesibles, en su caso, a las autoridades nacionales competentes suscita 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 (véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/12, EU:C:2014:238, apartados 25 y 70, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 91 y 92 y jurisprudencia citada).

114 Así pues, la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 debe tener en cuenta la importancia tanto del derecho al respeto de la vida privada, garantizado por el artículo 7 de la Carta, como del derecho a la protección de los datos personales, que garantiza el artículo 8 de esta, tal como se deriva de la jurisprudencia del Tribunal de Justicia, y la del derecho a la libertad de expresión, derecho fundamental, garantizado en el artículo 11 de la Carta, que constituye uno de los fundamentos esenciales de una sociedad democrática y pluralista, y forma parte de los valores en los que se basa la Unión, con arreglo al artículo 2 TUE (véanse, en este sentido, las sentencias de 6 de marzo de 2001, Connolly/Comisión, C-274/99 P, EU:C:2001:127, apartado 39, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 93 y jurisprudencia citada).

115 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, prevista 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, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126 y jurisprudencia citada; véase, por analogía, por lo que se refiere el artículo 8 del CEDH, TEDH, sentencia de 30 de enero de 2020, Breyer c. Alemania, CE:ECHR:2020:0130JUD005000112, § 81).

116 Carece asimismo de relevancia que los datos conservados se utilicen o no posteriormente (véanse, por analogía, por lo que se refiere al artículo 8 del CEDH, TEDH, sentencia de 16 de febrero de 2000, Amann c. Suiza, CE:ECHR:2000:0216JUD002779895, § 69, y de 13 de febrero de 2020, Trjakovski y Chipovski c. Macedonia del Norte, CE:ECHR:2020:0213JUD005320513, § 51), puesto que el acceso a tales datos constituye, cualquiera que sea la utilización posterior que se haga de ellos, una injerencia distinta en los derechos fundamentales mencionados en el apartado anterior [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126].

117 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 (véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/12, EU:C:2014:238, apartado 27, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 99).

118 En consecuencia, por una parte, la conservación de datos de tráfico y de datos de localización con fines policiales puede vulnerar en sí misma 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 en el artículo 11 de la Carta (véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/12, EU:C:2014:238, apartado 28, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 101). Pues bien, tales efectos disuasorios pueden afectar, en particular, a las personas cuyas comunicaciones estén sujetas, según las normas nacionales, al secreto profesional y a los denunciantes cuyas actividades estén protegidas por la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (DO 2019, L 305, p. 17). Además, estos efectos son especialmente graves, dada la cantidad y la variedad de datos conservados.

119 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.

120 Dicho esto, en la medida en que permite a los Estados miembros establecer las excepciones contempladas en el apartado 110 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 según su función en la sociedad (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 172 y jurisprudencia citada).

121 En efecto, como se desprende del artículo 52, apartado 1, de la Carta, esta admite limitaciones del ejercicio de estos derechos, siempre que esas limitaciones sean establecidas por la ley, respeten el contenido esencial de esos derechos y, dentro del respeto del principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

122 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 de 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.

123 A este respecto, el artículo 6 de la Carta, al que se refieren el Conseil d'État (Consejo de Estado) y la Cour constitutionnelle (Tribunal Constitucional), establece el derecho de todas las personas no solo a la libertad, sino también a la seguridad, y garantiza los derechos correspondientes a los garantizados por el artículo 5 del CEDH (véanse, en este sentido, las sentencias de 15 de febrero de 2016, N., C-601/15 PPU, EU:C:2016:84, apartado 47; de 28 de julio de 2016, JZ, C-294/16 PPU, EU:C:2016:610, apartado 48, y de 19 de septiembre de 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, apartado 42 y jurisprudencia citada).

124 Por otra parte, procede recordar que el artículo 52, apartado 3, de la Carta pretende garantizar la coherencia necesaria entre los derechos que contiene esta y los derechos correspondientes garantizados por el CEDH, sin que ello afecte a la autonomía del Derecho de la Unión y del Tribunal de Justicia de la Unión Europea. A efectos de la interpretación de la Carta, por tanto, procede tener en cuenta los derechos correspondientes del CEDH como nivel mínimo de protección [véanse, en este sentido, las sentencias de 12 de febrero de 2019, TC, C-492/18 PPU, EU:C:2019:108, apartado 57, y de 21 de mayo de 2019, Comisión/Hungría (Usufructos sobre terrenos agrícolas), C-235/17, EU:C:2019:432, apartado 72 y jurisprudencia citada].

125 En cuanto al artículo 5 del CEDH, que consagra el «derecho a la libertad» y el «derecho a la seguridad», este tiene por objeto, según la jurisprudencia del Tribunal Europeo de Derechos Humanos, proteger al individuo contra toda privación de libertad arbitraria o injustificada (véanse, en este sentido, TEDH, sentencia de 18 de marzo de 2008, Ladent c. Polonia, CE:ECHR:2008:0318JUD001103603, §§ 45 y 46; 29 de marzo de 2010, Medvedyev y otros c. Francia, CE:ECHR:2010:0329JUD000339403, §§ 76 y 77, y de 13 de diciembre de 2012, El-Masri c. «The former Yugoslav Republic of Macedonia», CE:ECHR:2012:1213JUD003963009, § 239). No obstante, en la medida en que esta disposición se refiere a una privación de libertad cometida por una autoridad pública, el artículo 6 de la Carta no puede interpretarse en el sentido de que obliga a los poderes públicos a adoptar medidas específicas para sancionar determinados delitos.

126 En cambio, por lo que respecta, específicamente, a la lucha efectiva contra los delitos perpetrados, en particular, contra los menores y otras personas vulnerables, mencionada por la Cour constitutionnelle (Tribunal Constitucional), es preciso subrayar 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 [véase, en este sentido, la sentencia de 18 de junio de 2020, Comisión/Hungría (Transparencia asociativa), C-78/18, EU:C:2020:476, apartado 123 y jurisprudencia citada del Tribunal Europeo de Derechos Humanos]. 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.

127 Pues bien, frente a estas diferentes obligaciones positivas, conviene proceder a una conciliación necesaria de los distintos intereses y derechos en juego.

128 En efecto, el Tribunal Europeo de Derechos Humanos ha declarado que las obligaciones positivas resultantes de los artículos 3 y 8 del CEDH, 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 y derechos que se han de proteger (TEDH, sentencia de 28 de octubre de 1998, Osman c. Reino Unido, CE:ECHR:1998:1028JUD002345294, §§ 115 y 116; de 4 de marzo de 2004, M. C. c. Bulgaria, CE:ECHR:2003:1204JUD003927298, § 151; de 24 de junio de 2004, Von Hannover c. Alemania, CE:ECHR:2004:0624JUD005932000, §§ 57 y 58, y de 2 de diciembre de 2008, K. U. c. Finlandia, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 y 49).

129 En lo que respecta al respeto del principio de proporcionalidad, el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 dispone que los Estados miembros podrán adoptar una medida que suponga una excepción al principio de confidencialidad de las comunicaciones y de los datos de tráfico relativos a ellas cuando esa medida sea «necesaria, proporcionada y apropiada en una sociedad democrática», a la vista de los objetivos que enuncia dicha disposición. El considerando 11 de esta Directiva precisa que una medida de esta naturaleza debe ser «rigurosamente» proporcionada al objetivo que pretende lograr.

130 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 [véanse, en este sentido, las sentencias de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 56; de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartados 76, 77 y 86, y de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/12, EU:C:2014:238, apartado 52; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 140].

131 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 (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 55 y jurisprudencia citada).

132 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 aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles [véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].

133 De este modo, una normativa 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 [véanse, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 191 y jurisprudencia citada, y la sentencia de 3 de octubre de 2019, A y otros, C-70/18, EU:C:2019:823, apartado 63].

– Sobre las medidas legislativas que establecen la conservación preventiva de los datos de tráfico y de los datos de localización para proteger la seguridad nacional

134 Procede observar que el objetivo de protección de la seguridad nacional, mencionado por los órganos jurisdiccionales remitentes y los Gobiernos que han presentado observaciones, aún no ha sido examinado específicamente por el Tribunal de Justicia en sus sentencias en las que interpreta la Directiva 2002/58.

135 A este respecto, debe señalarse, para empezar, que el artículo 4 TUE, apartado 2, establece que la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro. Esta responsabilidad corresponde al interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad e incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país, y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado, tales como las actividades terroristas.

136 Pues bien, la importancia del objetivo de protección de la seguridad nacional, interpretado a la luz del artículo 4 TUE, apartado 2, supera la de los demás objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, en particular de los objetivos de combatir la delincuencia en general, incluso grave, y de protección de la seguridad pública. En efecto, amenazas como las mencionadas en el apartado anterior se distinguen, por su naturaleza y especial gravedad, del riesgo general de que surjan tensiones o perturbaciones, incluso graves, que afecten a la seguridad pública. Por lo tanto, sin perjuicio del cumplimiento de los demás requisitos establecidos en el artículo 52, apartado 1, de la Carta, el objetivo de protección de la seguridad nacional puede justificar medidas que supongan injerencias en los derechos fundamentales más graves que las que podrían justificar esos otros objetivos.

137 Así, en situaciones como las descritas en los apartados 135 y 136 de la presente sentencia, el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y 52, apartado 1, de la Carta, no se opone, en principio, a una medida legislativa que autoriza a las autoridades competentes a instar a los proveedores de servicios de comunicaciones electrónicas a proceder a la conservación de los datos de tráfico y de los datos de localización del conjunto de los usuarios de los medios de comunicaciones electrónicas durante un período limitado, siempre que existan circunstancias suficientemente concretas que permitan considerar que el Estado miembro en cuestión se enfrenta a una amenaza grave, como la contemplada en los apartados 135 y 136 de la presente sentencia, para la seguridad nacional que resulte real y actual o previsible. Aun cuando dicha medida se refiera, de modo indiscriminado, a todos los usuarios de medios de comunicaciones electrónicas sin que estos parezcan, a primera vista, guardar relación, en el sentido de la

jurisprudencia citada en el apartado 133 de la presente sentencia, con una amenaza para la seguridad nacional de dicho Estado miembro, procede considerar que la existencia de dicha amenaza puede, por sí sola, establecer esa relación.

138 El requerimiento por el que se ordena la conservación preventiva de los datos del conjunto de los usuarios de los medios de comunicaciones electrónicas debe, no obstante, limitarse temporalmente a lo estrictamente necesario. Si bien no cabe excluir que, debido a la persistencia de dicha amenaza, pueda renovarse el requerimiento por el que se ordena a los proveedores de servicios de comunicaciones electrónicas conservar los datos, la duración de cada requerimiento no puede exceder de un período de tiempo previsible. Además, esta conservación de los datos debe estar sujeta a limitaciones y acompañarse de garantías estrictas que permitan proteger eficazmente los datos de carácter personal de las personas afectadas contra los riesgos de abuso. De esta forma, dicha conservación no puede tener carácter sistemático.

139 Habida cuenta de la gravedad de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que resulta de dicha medida de conservación generalizada e indiferenciada de los datos, es preciso garantizar que el recurso a la misma se limite efectivamente a las situaciones en las que existe una amenaza grave para la seguridad nacional, como las contempladas en los apartados 135 y 136 de la presente sentencia. A tal fin, es fundamental que una decisión por la que se inste a los proveedores de servicios de comunicaciones electrónicas a proceder a dicha conservación de los datos pueda ser objeto 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.

– Sobre las medidas legislativas que establecen la conservación preventiva de los datos de tráfico y de los datos de localización a efectos de la lucha contra la delincuencia y de la protección de la seguridad pública

140 En lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos, 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 [véanse, en este sentido, las sentencias de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 102, y de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartados 56 y 57; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 149].

141 Una normativa nacional que establece la conservación generalizada e indiferenciada de los datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave excede de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 107).

142 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, contemplados en el apartado 118 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.

143 Por otro lado, el Tribunal de Justicia ha subrayado 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. Dicha normativa, contrariamente a la exigencia recordada en el apartado 133 de la presente sentencia, 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 remota, 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 (véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/12, EU:C:2014:238, apartados 57 y 58, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 105).

144 En particular, como ya ha declarado el Tribunal de Justicia, dicha 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 (véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/12, EU:C:2014:238, apartado 59, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 106).

145 Pues bien, 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 los apartados 126 y 128 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.

146 En cambio, como se ha expuesto en los apartados 142 a 144 de la presente sentencia, y habida cuenta de la conciliación necesaria de los derechos e intereses en juego, los objetivos de lucha contra la delincuencia grave, de prevención de las amenazas graves a la seguridad pública y, *a fortiori*, de protección de la seguridad nacional pueden justificar, a la vista de su importancia, respecto de las obligaciones positivas recordadas en el apartado anterior y a las que se refiere concretamente la Cour constitutionnelle (Tribunal Constitucional), la injerencia especialmente grave que supone una conservación selectiva de los datos de tráfico y de localización.

147 De este modo, como ya ha declarado el Tribunal de Justicia, el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a que un Estado miembro adopte una normativa que permita, con carácter preventivo, una conservación selectiva de los datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave y de la prevención de las amenazas graves a la seguridad pública, así como a efectos de la protección de la seguridad nacional, siempre que dicha conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación

a que se refieran, las personas afectadas y el período de conservación establecido (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 108).

148 Por lo que se refiere a la delimitación de que debe ser objeto dicha medida de conservación de los datos, esta puede, en particular, fijarse en función de las categorías de personas afectadas, ya que el artículo 15, apartado 1, de la Directiva 2002/58 no se opone a una normativa basada en elementos objetivos, que permitan dirigirse a las personas cuyos datos de tráfico y de localización puedan presentar una relación, por lo menos indirecta, con delitos graves, contribuir de un modo u otro a la lucha contra la delincuencia grave o prevenir un riesgo grave para la seguridad pública, o incluso un riesgo para la seguridad nacional (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 111).

149 A este respecto, es preciso señalar que dichas personas pueden, en particular, ser aquellas que se han identificado previamente, en el marco de procedimientos nacionales aplicables y sobre la base de elementos objetivos, como una amenaza para la seguridad pública o la seguridad nacional del Estado miembro en cuestión.

150 La delimitación de una medida que establece la conservación de los datos de tráfico y de localización puede basarse asimismo en un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de elementos objetivos y no discriminatorios, que existe una situación caracterizada por un riesgo elevado de preparación o de comisión de tales delitos graves en una o varias zonas geográficas (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 111). Estas zonas pueden ser, en particular, lugares que cuentan con 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 o zonas de peajes.

151 A fin de garantizar que la injerencia que suponen las medidas de conservación selectiva descritas en los apartados 147 a 150 de la presente sentencia sea conforme con el principio de proporcionalidad, su duración 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.

– Sobre las medidas legislativas que establecen la conservación preventiva de las direcciones IP y de los datos relativos a la identidad civil a efectos de la lucha contra la delincuencia y de la protección de la seguridad pública

152 Es preciso señalar que las direcciones IP, pese a formar parte de los datos de tráfico, se generan sin estar vinculadas a una comunicación determinada y sirven fundamentalmente para identificar, por medio de los proveedores de servicios de comunicaciones electrónicas, a la persona física propietaria de un equipo terminal desde el que se efectúa una comunicación a través de Internet. De este modo, en materia de correo electrónico y de telefonía por internet, dado que las únicas direcciones IP que se conservan son las del origen de la comunicación y no las de su destinatario, dichas direcciones no revelan, como tales, ninguna información sobre las terceras personas que han estado en contacto con la persona que da origen a la comunicación. Por lo tanto, esta categoría de datos presenta un grado de sensibilidad menor que los demás datos de tráfico.

153 No obstante, puesto que las direcciones IP pueden utilizarse para llevar a cabo, en particular, el rastreo exhaustivo de la secuencia de navegación de un internauta y, en consecuencia, de su actividad en línea, tales datos permiten establecer el perfil detallado de este. Por lo tanto, la conservación y el análisis de

dichas direcciones IP que precisa ese rastreo constituyen injerencias graves en los derechos fundamentales del internauta consagrados en los artículos 7 y 8 de la Carta, que pueden tener efectos disuasorios como los contemplados en el apartado 118 de la presente sentencia.

154 Pues bien, a efectos de la conciliación necesaria de los derechos e intereses en juego exigida por la jurisprudencia citada en el apartado 130 de la presente sentencia, es preciso tener en cuenta el hecho de que, en el caso de un delito cometido en línea, 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. A esto se añade el hecho de que la conservación de las direcciones IP por parte de los proveedores de servicios de comunicaciones electrónicas más allá de la duración de atribución de tales datos no parece, en principio, necesaria para la facturación de los servicios de que se trate, de tal manera que la detección de los delitos cometidos en línea puede, en consecuencia, como han indicado varios Gobiernos en sus observaciones presentadas al Tribunal de Justicia, resultar imposible sin recurrir a una medida legislativa en virtud del artículo 15, apartado 1, de la Directiva 2002/58. Este puede ser el caso, en particular, como han afirmado estos Gobiernos, de los delitos especialmente graves en materia de pornografía infantil, como 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).

155 En estas circunstancias, si bien es cierto que una medida legislativa que establece la conservación de las direcciones IP del conjunto de las personas físicas propietarias de un equipo terminal desde el que puede accederse a internet se dirigiría a personas que a primera vista no presentan ninguna relación, en el sentido de la jurisprudencia citada en el apartado 133 de la presente sentencia, con los objetivos perseguidos y que, conforme a lo expuesto en el apartado 109 de la presente sentencia, los internautas tienen derecho a esperar, con arreglo a los artículos 7 y 8 de la Carta, que su identidad no sea, en principio, revelada, una medida legislativa que establece únicamente la conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión no parece, en principio, contraria al artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta, siempre que esta posibilidad esté sujeta al riguroso respeto de las condiciones materiales y procesales que deben regular la utilización de tales datos.

156 Habida cuenta del carácter grave de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que supone esta conservación, solo la lucha contra la delincuencia grave y la prevención de las amenazas graves a la seguridad pública pueden, al igual que la protección de la seguridad nacional, justificar esta injerencia. Además, la duración de conservación no puede exceder de lo estrictamente necesario habida cuenta del objetivo perseguido. Por último, una medida de esta naturaleza debe prever condiciones y garantías estrictas por lo que se refiere a la explotación de dichos datos, en particular mediante un rastreo, en lo que respecta a las comunicaciones y actividades efectuadas en línea por las personas afectadas.

157 En lo tocante, por último, a los datos relativos a la identidad civil de los usuarios de los medios de comunicaciones electrónicas, dichos datos no permiten, por sí solos, conocer la fecha, la hora, la duración y los destinatarios de las comunicaciones efectuadas, ni los lugares en los que se produjeron estas comunicaciones o la frecuencia de las mismas con ciertas personas durante un período de tiempo determinado, por lo que no facilitan, al margen de las coordenadas de estos, como sus direcciones, ninguna información sobre las comunicaciones transmitidas y, en consecuencia, sobre su vida privada. De este modo, la injerencia que supone la conservación de estos datos no puede, en principio, calificarse de grave (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartados 59 y 60).

158 De ello se sigue que, conforme a lo expuesto en el apartado 140 de la presente sentencia, las medidas legislativas relativas al tratamiento de estos datos como tales, en particular a su conservación y al acceso a los mismos con el único objetivo de identificar al usuario de que se trate, y sin que dichos datos puedan vincularse a informaciones relativas a las comunicaciones efectuadas, pueden estar justificadas por el objetivo de prevenir, investigar, descubrir y perseguir delitos en general, al que se refiere el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 62).

159 En estas circunstancias, habida cuenta de la conciliación necesaria de los derechos e intereses en juego y por las razones contempladas en los apartados 131 y 158 de la presente sentencia, procede considerar que, incluso cuando no existe ningún vínculo entre el conjunto de los usuarios de los medios de comunicaciones electrónicas y los objetivos perseguidos, el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta, no se opone a una medida legislativa que impone, sin fijar un plazo concreto, a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar los datos relativos a la identidad civil del conjunto de los usuarios de los medios de comunicaciones electrónicas con fines de prevención, investigación, descubrimiento y persecución de delitos, así como de protección de la seguridad pública, sin que sea necesario que los delitos o que las amenazas o los atentados a la seguridad pública sean graves.

– Sobre las medidas legislativas que establecen la conservación rápida de los datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave

160 En relación con los datos de tráfico y de localización tratados y almacenados por los proveedores de servicios de comunicaciones electrónicas sobre la base de los artículos 5, 6 y 9 de la Directiva 2002/58, o sobre la de las medidas legislativas adoptadas en virtud del artículo 15, apartado 1, de esta, descritas en los apartados 134 a 159 de la presente sentencia, procede señalar que estos datos deben, en principio, según el caso, eliminarse o hacerse anónimos al término de los plazos legales en los que deben tratarse y almacenarse con arreglo a las disposiciones nacionales de transposición de esta Directiva.

161 No obstante, durante el tratamiento y el 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 a 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.

162 A este respecto, es preciso indicar que el Convenio sobre la Ciberdelincuencia del Consejo de Europa de 23 de noviembre de 2001 (Serie de Tratados Europeos n.º 185), que fue firmado por los 27 Estados miembros y ratificado por 25 de ellos, y cuyo objetivo es facilitar la lucha contra la delincuencia que hace uso de las redes informáticas, prevé, en su artículo 14, que cada Parte adoptará para los fines de investigaciones o procedimientos penales específicos determinadas medidas relativas a los datos de tráfico ya almacenados, como la conservación rápida de dichos datos. En particular, el artículo 16, apartado 1, del citado Convenio establece que cada Parte adoptará las medidas legislativas que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de los datos de tráfico almacenados por medio de un sistema informático, en particular cuando existan razones para creer que estos datos resultan susceptibles de pérdida o de modificación.

163 En una situación como la contemplada en el apartado 161 de la presente sentencia, habida cuenta de la conciliación necesaria de los derechos e intereses en juego a que se refiere el apartado 130 de la presente sentencia, los Estados miembros pueden prever, en una normativa adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58, la posibilidad de instar, mediante una decisión de la

autoridad competente sujeta a un control jurisdiccional efectivo, a los proveedores de servicios de comunicaciones electrónicas a proceder, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan.

164 En la medida en que la finalidad de dicha 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. Además, para garantizar que la injerencia que supone una medida de este tipo se limite a lo estrictamente necesario, es preciso, por una parte, que la obligación de conservación ataña únicamente a los datos de tráfico y de localización que puedan contribuir a la investigación del delito grave o del atentado a la seguridad nacional de que se trate. Por otra parte, la duración de conservación de los datos debe limitarse a lo estrictamente necesario, si bien podrá ampliarse cuando las circunstancias y el objetivo perseguido por dicha medida lo justifiquen.

165 A este respecto, es importante precisar que dicha conservación rápida no debe limitarse a los datos de las personas sobre las que recae una sospecha concreta de haber cometido un delito o un atentado a la seguridad nacional. Respetando el marco establecido por el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y 52, apartado 1, de la Carta, y habida cuenta de las consideraciones que se exponen en el apartado 133 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 las 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 dicho delito o de dicho atentando contra la seguridad nacional, como los datos de la víctima del mismo, de su entorno social o profesional, o incluso de zonas geográficas determinadas, como los lugares en que se cometió y se preparó el delito o el atentado contra la seguridad nacional de que se trate. Además, el acceso de las autoridades competentes a los datos conservados de este modo debe efectuarse respetando los requisitos que se derivan de la jurisprudencia que ha interpretado la Directiva 2002/58 (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartados 118 a 121 y jurisprudencia citada).

166 Conviene asimismo añadir que, como se desprende concretamente de los apartados 115 y 133 de la presente sentencia, 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 solo puede estar justificado, en principio, por el objetivo de interés general para el que dicha conservación se impuso a estos proveedores. De ello se sigue, en particular, que el acceso a tales datos con fines de persecución y de sanción de un delito ordinario no puede concederse en ningún caso cuando su conservación esté justificada por el objetivo de lucha contra la delincuencia grave o, *a fortiori*, de protección de la seguridad nacional. En cambio, con arreglo al principio de proporcionalidad, con las precisiones aportadas en el apartado 131 de la presente sentencia, el acceso a los datos conservados con el fin de luchar contra la delincuencia grave puede, siempre que se respeten las condiciones materiales y procesales relativas a dicho acceso previstas en el apartado anterior, estar justificado por el objetivo de protección de la seguridad nacional.

167 A este respecto, los Estados miembros pueden prever en su normativa que el acceso a los datos de tráfico y de localización pueda, dentro del respeto de estas condiciones materiales y procesales, efectuarse con fines de lucha contra la delincuencia grave o de protección de la seguridad nacional cuando tales datos sean conservados por un proveedor de conformidad con los artículos 5, 6 y 9 o incluso con el artículo 15, apartado 1, de la Directiva 2002/58.

168 Habida cuenta de las consideraciones anteriores, procede responder a las primeras cuestiones prejudiciales planteadas en los asuntos C-511/18 y C-512/18, así como a las cuestiones prejudiciales primera y segunda planteadas en el asunto C-520/18, que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a medidas legislativas que establezcan, para los fines previstos en dicho artículo 15, apartado 1, con carácter preventivo, 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 y 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;

– que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las 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;

– que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;

– que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia y de la protección de la seguridad pública, una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y

– que permitan, a efectos de la lucha contra la delincuencia grave y, *a fortiori*, de la protección de la seguridad nacional, recurrir 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.

Cuestiones prejudiciales segunda y tercera planteadas en el asunto C-511/18

169 Mediante las cuestiones prejudiciales segunda y tercera planteadas en el asunto C-511/18, 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 y 11 y el artículo 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas aplicar en sus redes medidas que permitan, por una parte, el análisis automatizado y la recopilación en tiempo real de los datos de tráfico y de localización y, por otra parte, la recopilación en tiempo real de los datos técnicos relativos a la localización de los equipos terminales utilizados, sin que se prevea la información de las personas afectadas por estos tratamientos y estas recopilaciones.

170 El órgano jurisdiccional remitente precisa que las técnicas de recopilación de información previstas en los artículos L. 851-2 a L. 851-4 del CSI no implican, para los proveedores de servicios de comunicaciones electrónicas, una obligación específica de conservación de los datos de tráfico y de localización. Por lo que se refiere, en particular, al análisis automatizado previsto en el artículo L. 851-3 del CSI, dicho órgano jurisdiccional señala que este tratamiento tiene por objeto detectar, sobre la base de criterios definidos a estos efectos, conexiones que pueden suponer una amenaza terrorista. En cuanto a la recopilación en tiempo real contemplada en el artículo L. 851-2 del CSI, dicho órgano jurisdiccional observa que esta se refiere únicamente a una o varias personas previamente identificadas como sospechosas de estar relacionadas con una amenaza terrorista. Según este mismo órgano jurisdiccional, estas dos técnicas solo pueden aplicarse con fines de prevención del terrorismo y se refieren a los datos mencionados en los artículos L. 851-1 y R. 851-5 del CSI.

171 Con carácter preliminar, conviene precisar que el hecho de que, con arreglo al artículo L. 851-3 del CSI, el análisis automatizado que este prevé no permita, como tal, identificar a los usuarios cuyos datos son objeto de dicho análisis no se opone a que tales datos se califiquen de «datos de carácter personal». En efecto, dado que el procedimiento establecido en el apartado IV de dicha disposición permite identificar en una fase posterior a la persona o personas afectadas por los datos cuyo análisis automatizado ha puesto de relieve que puede existir una amenaza terrorista, todas las personas cuyos datos son objeto del análisis automatizado siguen siendo identificables a partir de tales datos. Pues bien, según la definición de los datos de carácter personal que figura en el artículo 4, punto 1, del Reglamento 2016/679, constituyen tales datos la información relativa, en particular, a una persona física identificable.

Sobre el análisis automatizado de los datos de tráfico y de localización

172 Del artículo L. 851-3 del CSI se desprende que el análisis automatizado que prevé se corresponde, en esencia, con un filtrado de la totalidad de los datos de tráfico y de localización conservados por los proveedores de servicios de comunicaciones electrónicas, efectuado por estos a solicitud de las autoridades nacionales competentes y en función de los parámetros establecidos por estas. De ello se sigue que todos los datos de los usuarios de los medios de comunicaciones electrónicas se verifican si se corresponden con dichos parámetros. Por consiguiente, ha de considerarse que este análisis automatizado implica, para los proveedores de servicios de comunicaciones electrónicas en cuestión, practicar, por cuenta de la autoridad competente, un tratamiento generalizado e indiferenciado que adopta la forma de una utilización por procedimiento automatizado, en el sentido del artículo 4, punto 2, del Reglamento 2016/679, que abarca el conjunto de los datos de tráfico y de localización de todos los usuarios de medios de comunicaciones electrónicas. Este tratamiento es independiente de la recopilación posterior de los datos relativos a las personas identificadas tras el análisis automatizado, recopilación que está autorizada sobre la base del artículo L. 851-3, IV, del CSI.

173 Pues bien, una normativa nacional que autoriza dicho análisis automatizado de los datos de tráfico y de localización establece una excepción a la obligación de principio, prevista en el artículo 5 de la Directiva 2002/58, de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos asociados a ellas. Dicha normativa también constituye una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, cualquiera que sea la utilización posterior que se haga de estos datos. Por último, con arreglo a la jurisprudencia citada en el apartado 118 de la presente sentencia, esta normativa puede tener efectos disuasorios en el ejercicio de la libertad de expresión consagrada en el artículo 11 de la Carta.

174 Además, la injerencia resultante de un análisis automatizado de los datos de tráfico y de localización, como la controvertida en los litigios principales, resulta especialmente grave puesto que abarca de manera generalizada e indiferenciada los datos de las personas que utilizan servicios de comunicaciones electrónicas. Esta constatación se impone tanto más cuanto que, como se desprende de las normativas nacionales controvertidas en los litigios principales, los datos objeto del análisis automatizado pueden revelar la naturaleza de la información consultada en línea. Por añadidura, este análisis automatizado se aplica de forma general al conjunto de las personas que utilizan medios de comunicaciones electrónicas y, en consecuencia, también a las personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con actividades terroristas.

175 En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

176 Por otra parte, para cumplir el requisito de proporcionalidad recordado en los apartados 130 y 131 de la presente sentencia, según el cual las excepciones a la protección de los datos personales y las restricciones a dicha protección deben establecerse sin sobrepasar los límites de lo estrictamente necesario, una normativa nacional que regula el acceso de las autoridades competentes a los datos de tráfico y de localización conservados debe respetar los requisitos que se derivan de la jurisprudencia citada en el apartado 132 de la presente sentencia. En particular, dicha normativa no puede limitarse a exigir que el acceso de las autoridades a los datos responda a la finalidad perseguida por dicha normativa, sino que debe establecer también los requisitos materiales y procedimentales que regulen la referida utilización [véase, por analogía, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 192 y jurisprudencia citada].

177 A este respecto, es preciso recordar que la injerencia especialmente grave que supone una conservación generalizada e indiferenciada de los datos de tráfico y de localización, a la que se refieren las consideraciones que figuran en los apartados 134 a 139 de la presente sentencia, así como la injerencia especialmente grave que constituye su análisis automatizado, solo pueden cumplir el requisito de proporcionalidad en aquellas situaciones en las que un Estado miembro se enfrenta a una amenaza grave para la seguridad nacional que resulta real y actual o previsible, y a condición de que la duración de dicha conservación se limite a lo estrictamente necesario.

178 En situaciones como las mencionadas en el apartado anterior, la aplicación de un análisis automatizado de los datos de tráfico y de localización del conjunto de los usuarios de medios de comunicaciones electrónicas, durante un período estrictamente limitado, puede considerarse justificada a la luz de los requisitos que se derivan del artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta.

179 Sentado lo anterior, a fin de garantizar que el recurso a dicha medida se limite efectivamente a lo estrictamente necesario para la protección de la seguridad nacional, y más concretamente para la prevención del terrorismo, es fundamental, con arreglo a lo afirmado en el apartado 139 de la presente

sentencia, que la decisión por la que se autorice el análisis automatizado pueda ser objeto 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 situación que justifique dicha medida y el respecto de las condiciones y de las garantías que deben establecerse.

180 A este respecto, debe precisarse que los modelos y criterios preestablecidos en los que se basa este tipo de tratamiento de datos deben ser, por una parte, específicos y fiables, de modo que permitan llegar a resultados que identifiquen individuos sobre los que podría recaer una sospecha razonable de participación en actividades terroristas y, por otra parte, no discriminatorios [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 172].

181 Por otra parte, es preciso recordar que todo análisis automatizado efectuado en función de modelos y criterios que se basen en la premisa de que el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, la salud o a la sexualidad de una persona podrían, por sí solos y con independencia del comportamiento individual de dicha persona, ser pertinentes en atención a la prevención del terrorismo vulneraría los derechos garantizados en los artículos 7 y 8 de la Carta, en relación con el artículo 21 de esta. De este modo, los modelos y criterios preestablecidos a efectos de un análisis automatizado que tenga por objeto prevenir actividades terroristas que presenten una amenaza grave para la seguridad nacional no pueden basarse únicamente en estos datos sensibles [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 165].

182 Además, puesto que los análisis automatizados de los datos de tráfico y de localización conllevan necesariamente cierto margen de error, cualquier resultado positivo obtenido gracias a un tratamiento automatizado debe reexaminarse individualmente por medios no automatizados antes de adoptar una medida individual que produzca efectos perjudiciales para las personas afectadas, como la recopilación posterior de los datos de tráfico y de localización en tiempo real, sin que una medida de este tipo pueda basarse, en efecto, de forma decisiva exclusivamente en el resultado de un tratamiento automatizado. De igual modo, para garantizar, en la práctica, que los modelos y criterios preestablecidos, el uso que se haga de ellos y las bases de datos utilizadas no tengan carácter discriminatorio y se limiten a lo estrictamente necesario atendiendo al objetivo de prevenir actividades terroristas que constituyan una amenaza grave para la seguridad nacional, la fiabilidad y la actualidad de esos modelos y criterios preestablecidos y de las bases de datos utilizadas deben ser objeto de un reexamen regular [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 173 y 174].

Sobre la recopilación en tiempo real de los datos de tráfico y de localización

183 En lo que atañe a la recopilación en tiempo real de los datos de tráfico y de localización a que se refiere el artículo L. 851-2 del CSI, es preciso señalar que esta puede autorizarse individualmente en lo que se refiere a «una persona previamente identificada como sospechosa de estar relacionada con una amenaza [terrorista]». De igual modo, según esta disposición, «cuando existan razones serias para considerar que una o varias personas pertenecientes al entorno de la persona respecto de la que se ha concedido la autorización pueden facilitar información en virtud de la finalidad que motiva la autorización, esta podrá concederse asimismo individualmente respecto de cada una de estas personas».

184 Los datos que constituyen el objeto de una medida de esta naturaleza permiten a las autoridades nacionales competentes vigilar, durante la vigencia de la autorización, de manera continua y en tiempo real, a los interlocutores con los que las personas afectadas se comunican, los medios que estas utilizan, la duración de sus comunicaciones y sus lugares de residencia y desplazamientos. Asimismo, pueden revelar la naturaleza de la información consultada en línea. Considerados en su conjunto, estos datos permiten, como se desprende del apartado 117 de la presente sentencia, extraer conclusiones muy

precisas sobre la vida privada de las personas afectadas y proporcionan los medios para determinar el perfil de las mismas, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones.

185 En cuanto a la recopilación de datos en tiempo real a que se refiere el artículo L. 851-4 del CSI, esta disposición autoriza la recopilación de los datos técnicos relativos a la localización de equipos terminales y la transmisión en tiempo real a un servicio del Primer Ministro. Parece que tales datos permiten al servicio competente, en cualquier momento durante la vigencia de la autorización, localizar, de manera continua y en tiempo real, equipos terminales utilizados, como teléfonos móviles.

186 Pues bien, una normativa nacional que autoriza dichas recopilaciones en tiempo real establece una excepción, al igual que la que autoriza el análisis automatizado de los datos, a la obligación de principio, prevista en el artículo 5 de la Directiva 2002/58, de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos asociados a ellas. Por lo tanto, dicha normativa también constituye una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta y puede tener efectos disuasorios en el ejercicio de la libertad de expresión consagrada en el artículo 11 de la Carta.

187 Es preciso subrayar que la injerencia que supone la recopilación en tiempo real de los datos que permiten localizar un equipo terminal parece especialmente grave, pues estos datos facilitan a las autoridades nacionales competentes un método de seguimiento preciso y continuo de los desplazamientos de los usuarios de los teléfonos móviles. En la medida en que cabe considerar, de este modo, estos datos como especialmente sensibles, el acceso en tiempo real de las autoridades competentes a dichos datos debe distinguirse de un acceso en tiempo diferido a los mismos, resultando el primero de ellos más intrusivo al permitir una vigilancia prácticamente perfecta de tales usuarios (véase, por analogía, por lo que se refiere al artículo 8 del CEDH, TEDH, sentencia 8 de febrero de 2018, Ben Faiza c. Francia, CE:ECHR:2018:0208JUD003144612, § 74). La intensidad de esta injerencia se ve, por otra parte, agravada cuando la recopilación en tiempo real se extiende asimismo a los datos de tráfico de las personas afectadas.

188 Aunque el objetivo de prevención del terrorismo que persigue la normativa nacional controvertida en los litigios principales puede, habida cuenta de su importancia, justificar la injerencia que supone la recopilación en tiempo real de los datos de tráfico y de localización, dicha medida solo puede aplicarse, teniendo en cuenta su carácter especialmente intrusivo, respecto de las personas de las que se sospeche fundadamente que están implicadas de un modo u otro en actividades terroristas. En cuanto a los datos de las personas que no están comprendidas en dicha categoría, estos únicamente pueden ser objeto de un acceso en tiempo diferido, que solo puede producirse, con arreglo a la jurisprudencia del Tribunal de Justicia, en situaciones particulares, como aquellas en las que se trate de actividades terroristas, y cuando existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra el terrorismo (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 119 y jurisprudencia citada).

189 Además, una decisión por la que se autorice la recopilación en tiempo real de los datos de tráfico y de localización debe basarse en criterios objetivos establecidos en la normativa nacional. En particular, dicha normativa debe definir, con arreglo a la jurisprudencia citada en el apartado 176 de la presente sentencia, las circunstancias y los requisitos conforme a los cuales puede autorizarse dicha recopilación y prever que, como se ha indicado en el apartado anterior, esta recopilación solo puede aplicarse a las personas que presenten una relación con el objetivo de prevención del terrorismo. Por otra parte, una decisión por la que se autorice la recopilación en tiempo real de los datos de tráfico y de localización debe basarse en criterios objetivos y no discriminatorios establecidos en la normativa nacional. Para garantizar en la práctica el cumplimiento de estos requisitos, es esencial que la aplicación de la medida por la que se autorice la recopilación en tiempo real esté sujeta a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa

independiente, cuya decisión tenga carácter vinculante, debiendo asegurarse dicho órgano o entidad, en particular, de que esta recopilación en tiempo real únicamente se autoriza dentro de los límites de lo estrictamente necesario (véase, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 120). En caso de urgencia debidamente justificada, el control debe efectuarse en breve plazo.

Sobre la información de las personas cuyos datos han sido recopilados o analizados

190 Es importante que las autoridades nacionales competentes que efectúen la recopilación en tiempo real de los datos de tráfico y de localización informen de ello a las personas afectadas, en el marco de los procedimientos nacionales aplicables, siempre que y a partir del momento en que dicha comunicación no pueda comprometer las misiones que corresponden a dichas autoridades. En efecto, esa información es, de hecho, necesaria para que dichas personas puedan ejercer su derecho, resultante de los artículos 7 y 8 de la Carta, a solicitar el acceso a sus datos de carácter personal objeto de dichas medidas y, en su caso, su rectificación o supresión, así como a interponer, con arreglo al artículo 47, párrafo primero, de la Carta, un recurso efectivo ante un tribunal, derecho que está, además, expresamente garantizado en el artículo 15, apartado 2, de la Directiva 2002/58, en relación con el artículo 79, apartado 1, del Reglamento 2016/679 [véanse, en este sentido, la sentencia de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 121 y jurisprudencia citada, y el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 219 y 220].

191 En cuanto a la información necesaria en el contexto de un análisis automatizado de los datos de tráfico y de localización, la autoridad nacional competente tiene la obligación de publicar información de carácter general relativa a dicho análisis, sin tener que informar individualmente a las personas afectadas. En cambio, en el supuesto de que los datos respondan a los parámetros precisos en la medida en que autorizan el análisis automatizado o de que dicha autoridad proceda a identificar a la persona afectada para analizar más en profundidad los datos que la conciernen, la información individual de esta persona resulta necesaria. No obstante, únicamente debe procederse a esa información siempre que y a partir del momento en que no pueda comprometer las misiones que corresponden a dicha autoridad [véase, por analogía, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 222 a 224].

192 Habida cuenta del conjunto de consideraciones anteriores, procede responder a las cuestiones prejudiciales segunda y tercera planteadas en el asunto C-511/18 que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta, debe interpretarse en el sentido de que no se opone a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de recurrir, por una parte, al análisis automatizado y a la recopilación en tiempo real, en particular, de los datos de tráfico y de localización y, por otra parte, a la recopilación en tiempo real de los datos técnicos relativos a la localización de los equipos terminales utilizados, cuando

– el recurso al análisis automatizado se limite a aquellas situaciones en las que un Estado miembro se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, pudiendo ser objeto el recurso a dicho análisis 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 situación que justifique dicha medida, así como el respecto de las condiciones y de las garantías que deben establecerse, y

– el recurso a una recopilación en tiempo real de los datos de tráfico y de localización se limite a las personas de las que se sospeche fundadamente que están implicadas de un modo u otro en actividades terroristas y esté sujeto a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter

vinculante, con el fin de garantizar que dicha recopilación en tiempo real únicamente se autoriza dentro de los límites de lo estrictamente necesario. En caso de urgencia debidamente justificada, el control debe efectuarse en breve plazo.

Segunda cuestión prejudicial planteada en el asunto C-512/18

193 Mediante la segunda cuestión prejudicial planteada en el asunto C-512/18, el órgano jurisdiccional remitente solicita, en esencia, que se dilucide si las disposiciones de la Directiva 2000/31, en relación con los artículos 6 a 8 y 11 y el artículo 52, apartado 1, de la Carta, deben interpretarse en el sentido de que se oponen a una normativa nacional que impone a los proveedores de acceso a los servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento la obligación de proceder a la conservación generalizada e indiferenciada, en particular, de los datos de carácter personal correspondientes a estos servicios.

194 Si bien considera que estos servicios están comprendidos en el ámbito de aplicación de la Directiva 2000/31, y no en el de la Directiva 2002/58, el órgano jurisdiccional remitente estima que el artículo 15, apartados 1 y 2, de la Directiva 2000/31, en relación con sus artículos 12 y 14, no establece, por sí solo, una prohibición de principio de conservar los datos relativos a la creación de contenido, a la que únicamente cabría establecer excepciones. Dicho órgano jurisdiccional se pregunta, no obstante, si esta apreciación debe realizarse habida cuenta del respeto necesario de los derechos fundamentales consagrados en los artículos 6 a 8 y 11 de la Carta.

195 Además, el órgano jurisdiccional remitente precisa que su cuestión prejudicial se refiere a la obligación de conservación prevista en el artículo 6 de la LCEN, en relación con el Decreto n.º 2011-219. Los datos que los proveedores de servicios en cuestión deben conservar a este respecto incluyen, en particular, los datos relativos a la identidad civil de las personas que han utilizado dichos servicios, como su apellido, nombre, sus direcciones postales asociadas, sus direcciones de correo electrónico o de cuenta asociadas, sus contraseñas y, cuando la suscripción del contrato o de la cuenta sea de pago, el tipo de pago utilizado, la referencia del pago, el importe y la fecha y la hora de la transacción.

196 De igual modo, los datos a que se refiere la obligación de conservación comprenden los identificadores de los abonados, de las conexiones y de los equipos terminales utilizados, los identificadores atribuidos a los contenidos, las fechas y horas de inicio y de fin de las conexiones y de las operaciones, así como los tipos de protocolos utilizados para la conexión al servicio y para la transferencia de contenidos. El acceso a estos datos, cuya duración de conservación es de un año, puede solicitarse en el marco de procedimientos penales y civiles, para que se respeten las normas en materia de responsabilidad civil o penal, así como en el marco de medidas de recopilación de información a las que se aplica el artículo L. 851-1 del CSI.

197 A este respecto, es preciso señalar que, con arreglo a su artículo 1, apartado 2, la Directiva 2000/31 aproxima entre sí determinadas disposiciones nacionales aplicables a los servicios de la sociedad de la información previstos en su artículo 2, letra a).

198 Estos servicios abarcan, en efecto, los servicios que se prestan a distancia a través de equipos electrónicos de tratamiento y de almacenamiento de datos, a petición individual de un destinatario de servicios y, normalmente, a cambio de una remuneración, como los servicios de acceso a Internet o a una red de comunicación, así como los servicios de almacenamiento (véanse, en este sentido, las sentencias de 24 de noviembre de 2011, Scarlet Extended, C-70/10, EU:C:2011:771, apartado 40; de 16 de febrero de 2012, SABAM, C-360/10, EU:C:2012:85, apartado 34; de 15 de septiembre de 2016, Mc Fadden, C-484/14, EU:C:2016:689, apartado 55, y de 7 de agosto de 2018, SNB-REACT, C-521/17, EU:C:2018:639, apartado 42 y jurisprudencia citada).

199 No obstante, el artículo 1, apartado 5, de la Directiva 2000/31 dispone que esta no se aplicará a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46 y 97/66. A este respecto, de los considerandos 14 y 15 de la Directiva 2000/31 se desprende que la protección de la confidencialidad de las comunicaciones y de las personas físicas en lo que respecta al tratamiento de datos personales en el marco de los servicios de la sociedad de la información se rige únicamente por las Directivas 95/46 y 97/66, Directiva esta última que prohíbe, en su artículo 5, a efectos de la protección de la confidencialidad de las comunicaciones, cualquier forma de interceptar o vigilar las comunicaciones.

200 Así, las cuestiones relacionadas con la protección de la confidencialidad de las comunicaciones y de los datos de carácter personal deben apreciarse a la luz de la Directiva 2002/58 y del Reglamento 2016/679, que sustituyeron, respectivamente, a la Directiva 97/66 y a la Directiva 95/46, habida cuenta de que la protección que tiene por objeto garantizar la Directiva 2000/31 no puede, en cualquier caso, ir en perjuicio de las exigencias resultantes de la Directiva 2002/58 y del Reglamento 2016/679 (véase, en este sentido, la sentencia de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartado 57).

201 La obligación impuesta por la normativa nacional contemplada en el apartado 195 de la presente sentencia a los proveedores de servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento de conservar los datos de carácter personal relativos a estos servicios debe, en consecuencia, como ha observado, en esencia, el Abogado General en el punto 141 de sus conclusiones presentadas en los asuntos acumulados La Quadrature du Net y otros (C-511/18 y C-512/18, EU:C:2020:6), apreciarse a la luz de la Directiva 2002/58 o del Reglamento 2016/679.

202 De este modo, en función de si la prestación de los servicios cubiertos por esta normativa nacional está comprendida o no en el ámbito de aplicación de la Directiva 2002/58, estará regulada bien por esta última Directiva, en particular por su artículo 15, apartado 1, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta, bien por el Reglamento 2016/679, en particular por su artículo 23, apartado 1, en relación con las mismas disposiciones de la Carta.

203 En el presente asunto, no cabe excluir, como ha señalado la Comisión Europea en sus observaciones escritas, que algunos de los servicios a los que se aplica la normativa nacional contemplada en el apartado 195 de la presente sentencia constituyan servicios de comunicaciones electrónicas, en el sentido de la Directiva 2002/58, extremo que corresponde comprobar al órgano jurisdiccional remitente.

204 A este respecto, es preciso señalar que la Directiva 2002/58 cubre los servicios de comunicaciones electrónicas que cumplen los requisitos previstos en el artículo 2, letra c), de la Directiva 2002/21, al que se remite el artículo 2 de la Directiva 2002/58 y que define el servicio de comunicaciones electrónicas como «el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión». Por lo que se refiere a los servicios de la sociedad de la información, contemplados en los apartados 197 y 198 de la presente sentencia y cubiertos por la Directiva 2000/31, estos constituyen servicios de comunicaciones electrónicas cuando consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas (véase, en este sentido, la sentencia de 5 de junio de 2019, Skype Communications, C-142/18, EU:C:2019:460, apartados 47 y 48).

205 Así, los servicios de acceso a internet, que parecen estar cubiertos por la normativa nacional contemplada en el apartado 195 de la presente sentencia, constituyen, como confirma el considerando 10 de la Directiva 2002/21, servicios de comunicaciones electrónicas, en el sentido de dicha Directiva (véase, en este sentido, la sentencia de 5 de junio de 2019, Skype Communications, C-142/18, EU:C:2019:460, apartado 37). Este es también el caso de los servicios de mensajería por internet,

respecto de los que no parece que pueda excluirse que están comprendidos asimismo en el ámbito de aplicación de dicha normativa nacional, puesto que, desde un punto de vista técnico, implican, en su totalidad o principalmente, el transporte de señales a través de redes de comunicaciones electrónicas (véase, en este sentido, la sentencia de 13 de junio de 2019, Google, C-193/18, EU:C:2019:498, apartados 35 y 38).

206 Por lo que se refiere a los requisitos que se derivan del artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta, procede remitirse al conjunto de las constataciones y de las apreciaciones efectuadas en el marco de la respuesta dada a las primeras cuestiones prejudiciales planteadas en los asuntos C-511/18 y C-512/18, así como a las cuestiones prejudiciales primera y segunda planteadas en el asunto C-520/18.

207 En cuanto a los requisitos que se derivan del Reglamento 2016/679, es preciso recordar que este tiene como finalidad, en particular, tal y como se desprende de su considerando 10, garantizar un nivel elevado de protección de las personas físicas dentro de la Unión y, a tal efecto, garantizar en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de esas personas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 101).

208 A tal fin, todo tratamiento de datos personales debe, sin perjuicio de las excepciones admitidas al amparo del artículo 23 del Reglamento 2016/679, respetar los principios que regulan el tratamiento de los datos de carácter personal, así como los derechos de la persona afectada previstos, respectivamente, en los capítulos II y III de dicho Reglamento. En particular, todo tratamiento de datos de carácter personal debe, por una parte, ser conforme con los principios establecidos en el artículo 5 de dicho Reglamento y, por otra parte, cumplir las condiciones de licitud enumeradas en el artículo 6 del mismo Reglamento (véase, por analogía, por lo que se refiere a la Directiva 95/46, la sentencia de 30 de mayo de 2013, Worten, C-342/12, EU:C:2013:355, apartado 33 y jurisprudencia citada).

209 En lo que atañe, más concretamente, al artículo 23, apartado 1, del Reglamento 2016/679, procede señalar que este, a semejanza de lo que se halla previsto en el artículo 15, apartado 1, de la Directiva 2002/58, permite a los Estados miembros limitar, en relación con los fines que prevé y mediante medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en el mismo «cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar» la finalidad perseguida. Toda medida legislativa adoptada sobre esta base debe, en particular, respetar los requisitos específicos previstos en el artículo 23, apartado 2, de dicho Reglamento.

210 Así, no cabe interpretar el artículo 23, apartados 1 y 2, del Reglamento 2016/679 en el sentido de que puede conferir a los Estados miembros la facultad de menoscabar el respeto de la vida privada, infringiendo el artículo 7 de la Carta, así como las demás garantías previstas por esta (véase, por analogía, por lo que se refiere a la Directiva 95/46, la sentencia de 20 de mayo de 2003, Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartado 91). En particular, al igual que ocurre con el artículo 15, apartado 1, de la Directiva 2002/58, la facultad que el artículo 23, apartado 1, del Reglamento 2016/679 confiere a los Estados miembros solo puede ejercerse respetando la exigencia de proporcionalidad, según la cual las excepciones a la protección de los datos personales y las restricciones a dicha protección deben establecerse sin sobrepasar los límites de lo estrictamente necesario (véase, por analogía, por lo que se refiere a la Directiva 95/46, la sentencia de 7 de noviembre de 2013, IPI, C-473/12, EU:C:2013:715, apartado 39 y jurisprudencia citada).

211 De ello se sigue que las constataciones y de las apreciaciones efectuadas en el marco de la respuesta dada a las primeras cuestiones prejudiciales planteadas en los asuntos C-511/18 y C-512/18, así como a las cuestiones prejudiciales primera y segunda planteadas en el asunto C-520/18, se aplican *mutatis mutandis* al artículo 23 del Reglamento 2016/679.

212 Habida cuenta de las consideraciones anteriores, procede responder a la segunda cuestión prejudicial planteada en el asunto C-512/18 que la Directiva 2000/31 debe interpretarse en el sentido de que no es aplicable en materia de protección de la confidencialidad de las comunicaciones y de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal en el marco de los servicios de la sociedad de la información, puesto que dicha protección está regulada, según el caso, por la Directiva 2002/58 o por el Reglamento 2016/679. El artículo 23, apartado 1, del Reglamento 2016/679, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que impone a los proveedores de acceso a los servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento la obligación de proceder a la conservación generalizada e indiferenciada, en particular, de los datos de carácter personal correspondientes a estos servicios.

Tercera cuestión prejudicial planteada en el asunto C-520/18

213 Mediante la tercera cuestión prejudicial planteada en el asunto C-520/18, el órgano jurisdiccional remitente solicita que se dilucide, en esencia, si un órgano jurisdiccional nacional puede aplicar una disposición de su Derecho nacional que le faculta para limitar en el tiempo los efectos de una declaración de ilegalidad que le corresponde efectuar, con arreglo a ese Derecho, con respecto a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas, con miras, en particular, a la consecución de los objetivos de protección de la seguridad nacional y de lucha contra la delincuencia, una obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización, resultante de su carácter incompatible con el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta.

214 El principio de primacía del Derecho de la Unión consagra la preeminencia del Derecho de la Unión sobre el Derecho de los Estados miembros. Por consiguiente, este principio impone la obligación de garantizar la plena eficacia de las distintas normas de la Unión a todos los órganos e instituciones de los Estados miembros, sin que el Derecho de los Estados miembros pueda afectar a la eficacia reconocida a esas distintas normas en el territorio de dichos Estados [sentencias de 15 de julio de 1964, Costa, 6/64, EU:C:1964:66, pp. 1159 y 1160, y 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 y 158 y jurisprudencia citada].

215 En virtud del principio de primacía, 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 tales disposiciones, 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 [sentencias de 22 de junio de 2010, Melki y Abdeli, C-188/10 y C-189/10, EU:C:2010:363, apartado 43 y jurisprudencia citada; de 24 de junio de 2019, Popławski, C-573/17, EU:C:2019:530, apartado 58, y 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, apartado 160].

216 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 [véanse, en este sentido, las sentencias de 23 de octubre de 2012, Nelson y otros, C-581/10 y C-629/10, EU:C:2012:657, apartados 89 y 91; de 23 de abril de 2020, Herst, C-401/18, EU:C:2020:295, apartados 56 y 57, y de 25 de junio de 2020, A y otros (Éoliennes à Aalter y à Nevele), C-24/19, EU:C:2020:503, apartado 84 y jurisprudencia citada].

217 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 (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, apartado 177 y jurisprudencia citada).

218 No obstante, el Tribunal de Justicia ha declarado, en un asunto en el que se estaba examinando la legalidad de medidas adoptadas incumpliendo la obligación establecida 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 dichas medidas cuando ese mantenimiento esté 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, teniendo en cuenta que 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).

219 Pues bien, contrariamente al incumplimiento de una obligación procesal como la evaluación previa de las repercusiones de un proyecto 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 y 11 y el artículo 52, apartado 1, de la Carta, no puede ser objeto de una regularización mediante un procedimiento comparable al mencionado en el apartado anterior. En efecto, el mantenimiento de los efectos de una normativa nacional, como la controvertida en los litigios principales, 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.

220 Por tanto, el órgano jurisdiccional remitente no puede aplicar una disposición de su Derecho nacional que le faculta para limitar en el tiempo los efectos de una declaración de ilegalidad que le corresponde efectuar, con arreglo a ese Derecho, con respecto a la normativa nacional controvertida en el litigio principal.

221 Dicho esto, en sus observaciones presentadas al Tribunal de Justicia, VZ, WY y XX alegan que la tercera cuestión prejudicial suscita, implícita pero necesariamente, el problema de si el Derecho de la Unión se opone a un uso, en el marco de un proceso penal, de la información y de las pruebas que se han obtenido mediante una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con este Derecho.

222 A este respecto y al objeto de facilitar una respuesta útil al órgano jurisdiccional remitente, procede recordar que, en el estado actual del Derecho de la Unión, incumbe en principio únicamente al Derecho nacional determinar las normas relativas a la admisibilidad y a la apreciación, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia grave, de la información y de las pruebas que se han obtenido mediante dicha conservación de datos contraria al Derecho de la Unión.

223 En efecto, según reiterada jurisprudencia, ante la inexistencia de normas de la Unión en la materia, corresponde al ordenamiento jurídico interno de cada Estado miembro, en virtud del principio de autonomía procesal, configurar la regulación procesal de los recursos destinados a garantizar la salvaguardia de los derechos que el Derecho de la Unión confiere a los justiciables, a condición, sin embargo, de que no sean menos favorables que las que rigen situaciones similares de carácter interno (principio de equivalencia) y de que no hagan imposible en la práctica o excesivamente difícil el ejercicio de los derechos conferidos por el Derecho de la Unión (principio de efectividad) (véanse, en

este sentido, las sentencias de 6 de octubre de 2015, Târşia, C-69/14, EU:C:2015:662, apartados 26 y 27; de 24 de octubre de 2018, XC y otros, C-234/17, EU:C:2018:853, apartados 21 y 22 y jurisprudencia citada, y de 19 de diciembre de 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, apartado 33).

224 Por lo que se refiere al principio de equivalencia, corresponde al juez nacional que conoce de un procedimiento penal basado en informaciones o pruebas obtenidas incumpliendo los requisitos derivados de la Directiva 2002/58 comprobar si el Derecho nacional que rige dicho procedimiento prevé normas menos favorables por lo que se refiere a la admisibilidad y al uso de esas informaciones y pruebas que las que rigen las informaciones y las pruebas obtenidas vulnerando el Derecho interno.

225 En lo que atañe al principio de efectividad, es preciso señalar que las normas nacionales relativas a la admisibilidad y al uso de las informaciones y de las pruebas tienen como objetivo, en virtud de las elecciones efectuadas por el Derecho nacional, evitar que las informaciones y pruebas que se han obtenido de manera ilegal perjudiquen indebidamente a una persona sospechosa de haber cometido delitos. Pues bien, con arreglo al Derecho nacional, este objetivo puede alcanzarse, además de mediante una prohibición de utilizar dichas informaciones y pruebas, mediante normas y prácticas nacionales que regulen la apreciación y la ponderación de las informaciones y de las pruebas, o incluso mediante la consideración de su carácter ilegal en el marco de la determinación de la pena.

226 Sentado lo anterior, de la jurisprudencia del Tribunal de Justicia se desprende que la necesidad de excluir las informaciones y las pruebas obtenidas incumpliendo lo dispuesto en el Derecho de la Unión debe apreciarse atendiendo, en particular, al riesgo que la admisibilidad de dichas informaciones y pruebas supone para el respeto del principio de contradicción y, por lo tanto, del derecho a un juicio justo (véase, en este sentido, la sentencia de 10 de abril de 2003, Steffensen, C-276/01, EU:C:2003:228, apartados 76 y 77). Pues bien, un órgano jurisdiccional que considera que una parte no está en condiciones de comentar eficazmente un medio de prueba que pertenece a un ámbito que escapa al conocimiento de los jueces y puede influir destacadamente en la apreciación de los hechos debe declarar que existe una violación del derecho a un juicio justo y excluir ese medio de prueba a fin de evitar una violación de esta índole (véase, en este sentido, la sentencia de 10 de abril de 2003, Steffensen, C-276/01, EU:C:2003:228, apartados 78 y 79).

227 En consecuencia, el principio de efectividad exige al juez penal nacional que descarte las informaciones y las pruebas que se han obtenido a través de una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia, cuando estas personas no estén en condiciones de comentar eficazmente tales informaciones y pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y pueden influir destacadamente en la apreciación de los hechos.

228 Habida cuenta de las consideraciones anteriores, procede responder a la tercera cuestión prejudicial planteada en el asunto C-520/18 que un órgano jurisdiccional nacional no puede aplicar una disposición de su Derecho nacional que le faculta para limitar en el tiempo los efectos de una declaración de ilegalidad que le corresponde efectuar, con arreglo a ese Derecho, con respecto a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas, con miras, en particular, a la protección de la seguridad nacional y de lucha contra la delincuencia, una obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y artículo 52, apartado 1, de la Carta. Dicho artículo 15, apartado 1, interpretado a la luz del principio de efectividad, exige al juez penal nacional que descarte las informaciones y las pruebas que se han obtenido a través de una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia, cuando estas personas no estén

en condiciones de comentar eficazmente tales informaciones y pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y pueden influir destacadamente en la apreciación de los hechos.

Costas

229 Dado que el procedimiento tiene, para las partes de los litigios principales, el carácter de un incidente promovido ante los órganos jurisdiccionales remitentes, corresponde a estos resolver sobre las costas. Los gastos efectuados por quienes, no siendo partes de los litigios principales, 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 y 11 y con el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que se opone a medidas legislativas que establezcan, para los fines previstos en dicho artículo 15, apartado 1, con carácter preventivo, una conservación generalizada e indiferenciada de los datos de tráfico y de localización. En cambio, dicho 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 y 11 y el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales, 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;**

   – **que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las 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;**

   – **que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;**

– **que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia y de la protección de la seguridad pública, una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y**

– **que permitan, a efectos de la lucha contra la delincuencia grave y, *a fortiori*, de la protección de la seguridad nacional, recurrir 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 y 11 y el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales, debe interpretarse en el sentido de que no se opone a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de recurrir, por una parte, al análisis automatizado y a la recopilación en tiempo real, en particular, de los datos de tráfico y de localización y, por otra parte, a la recopilación en tiempo real de los datos técnicos relativos a la localización de los equipos terminales utilizados, cuando**

– **el recurso al análisis automatizado se limite a aquellas situaciones en las que un Estado miembro se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, pudiendo ser objeto el recurso a dicho análisis 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 situación que justifique dicha medida, así como el respecto de las condiciones y de las garantías que deben establecerse, y**

– **el recurso a una recopilación en tiempo real de los datos de tráfico y de localización se limite a las personas de las que se sospeche fundadamente que están implicadas de un modo u otro en actividades terroristas y esté sujeto a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, con el fin de garantizar que dicha recopilación en tiempo real únicamente se autoriza dentro de los límites de lo estrictamente necesario. En caso de urgencia debidamente justificada, el control debe efectuarse en breve plazo.**

3) **La Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), debe interpretarse en el sentido de que no es aplicable en materia de protección de la confidencialidad de las comunicaciones y de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal en el marco de los servicios de la sociedad de la información, puesto que dicha protección está regulada, según el caso, por la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, o por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46. El artículo 23, apartado 1, del Reglamento 2016/679, en relación con los artículos 7, 8 y 11 y el artículo 52,**

apartado 1, de la Carta de los Derechos Fundamentales, debe interpretarse en el sentido de que se opone a una normativa nacional que impone a los proveedores de acceso a los servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento la obligación de proceder a la conservación generalizada e indiferenciada, en particular, de los datos de carácter personal correspondientes a estos servicios.

4) **Un órgano jurisdiccional nacional no puede aplicar una disposición de su Derecho nacional que le faculta para limitar en el tiempo los efectos de una declaración de ilegalidad que le corresponde efectuar, con arreglo a ese Derecho, con respecto a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas, con miras, en particular, a la protección de la seguridad nacional y de lucha contra la delincuencia, una obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales. Dicho artículo 15, apartado 1, interpretado a la luz del principio de efectividad, exige al juez penal nacional que descarte las informaciones y las pruebas que se han obtenido a través de una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia, cuando estas personas no estén en condiciones de comentar eficazmente tales informaciones y pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y pueden influir destacadamente en la apreciación de los hechos.**

Firmas