Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Pleno)

de 30 de abril de 2024*

Índice

* Lengua de procedimiento: francés.

«Procedimiento prejudicial — Tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Confidencialidad de las comunicaciones electrónicas — Protección — Artículos 5 y 15, apartado 1 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8, 11 y 52, apartado 1 — Legislación nacional que tiene como finalidad luchar, a través de la acción de una autoridad pública, contra las vulneraciones del derecho de propiedad intelectual cometidas en Internet — "Procedimiento de respuesta gradual" — Recogida inicial, por organizaciones de titulares de derechos, de las direcciones IP utilizadas para actividades que vulneran los derechos de autor o los derechos afines a los derechos de autor — Acceso posterior de la autoridad pública encargada de proteger los derechos de autor y los derechos afines a los derechos de autor a datos de identidad civil correspondientes a esas direcciones IP conservadas por los proveedores de servicios de comunicaciones electrónicas — Tratamiento automatizado — Exigencia de control previo por un órgano jurisdiccional o una entidad administrativa independiente — Requisitos materiales y procedimentales — Garantías contra los riesgos de abuso y contra cualquier acceso y uso ilícitos de esos datos»

En el asunto C-470/21,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia), mediante resolución de 5 de julio de 2021, recibida en el Tribunal de Justicia el 30 de julio de 2021, en el procedimiento entre

La Quadrature du Net,

Fédération des fournisseurs d'accès à Internet associatifs,

Franciliens.net,

French Data Network

y

Premier ministre,

Ministre de la Culture,

EL TRIBUNAL DE JUSTICIA (Pleno),

integrado por el Sr. K. Lenaerts, Presidente, el Sr. L. Bay Larsen, Vicepresidente, el Sr. A. Arabadjiev, las Sras. A. Prechal (Ponente) y K. Jürimäe y los Sres. C. Lycourgos, E. Regan, T. von Danwitz, F. Biltgen, N. Piçarra y Z. Csehi, Presidentes de Sala, y los Sres. M. Ilešič, J.-C. Bonichot, S. Rodin y P. G. Xuereb, la Sra. L. S. Rossi, los Sres. I. Jarukaitis, A. Kumin, N. Jääskinen y N. Wahl, la Sra. I. Ziemele, los Sres. J. Passer y D. Gratsias, la Sra. M. L. Arastey Sahún y el Sr. M. Gavalec, Jueces;

Abogado General: Sr. M. Szpunar;

Secretarias: Sras. V. Giacobbo y M. Krausenböck, administradoras;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 5 de julio de 2022;

consideradas las observaciones presentadas:

– en nombre de La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net y French Data Network, por el Sr. A. Fitzjean Ó Cobhthaigh, avocat;

– en nombre del Gobierno francés, por las Sras. A. Daniel y A.-L. Desjonquères y por el Sr. J. Illouz, en calidad de agentes;

– en nombre del Gobierno danés, por las Sras. J. F. Kronborg y V. Pasternak Jørgensen, en calidad de agentes;

– en nombre del Gobierno estonio, por la Sra. M. Kriisa, en calidad de agente;

– en nombre del Gobierno finlandés, por la Sra. H. Leppo, en calidad de agente;

– en nombre del Gobierno sueco, por la Sra. H. Shev, en calidad de agente;

– en nombre del Gobierno noruego, por los Sres. F. Bergsjø y S.-E. Dahl, la Sra. J. T. Kaasin y el Sr. P. Wennerås, en calidad de agentes;

– en nombre de la Comisión Europea, por los Sres. S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal y F. Wilman, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 27 de octubre de 2022;

visto el auto de reapertura de la fase oral de 23 de marzo de 2023 y celebrada la vista el 15 de mayo de 2023;

consideradas las observaciones presentadas:

– en nombre de La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net y French Data Network, por el Sr. A. Fitzjean Ó Cobhthaigh, avocat;

– en nombre del Gobierno francés, por los Sres. R. Bénard, J. Illouz y T. Stéhelin, en calidad de agentes;

– en nombre del Gobierno checo, por la Sra. T. Suchá y el Sr. J. Vláčil, en calidad de agentes;

– en nombre del Gobierno danés, por las Sras. J. F. Kronborg y C. A.-S. Maertens, en calidad de agentes;

– en nombre del Gobierno estonio, por la Sra. M. Kriisa, en calidad de agente;

– en nombre de Irlanda, por la Sra. M. Browne, Chief State Solicitor, y los Sres. A. Joyce y D. O'Reilly, en calidad de agentes, asistidos por el Sr. D. Fennelly, BL;

– en nombre del Gobierno español, por la Sra. A. Gavela Llopis, en calidad de agente;

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

– en nombre del Gobierno letón, por las Sras. J. Davidoviča y K. Pommere, en calidad de agentes;

– en nombre del Gobierno neerlandés, por las Sras. E. M. M. Besselink, M. K. Bultermann y A. Hanje, en calidad de agentes;

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

– en nombre del Gobierno sueco, por las Sras. F.-D. Göransson y H. Shev, en calidad de agentes;

– en nombre del Gobierno noruego, por los Sres. S.-E. Dahl y P. Wennerås, en calidad de agentes;

– en nombre de la Comisión Europea, por los Sres. S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal y F. Wilman, en calidad de agentes;

– en nombre del Supervisor Europeo de Protección de Datos, por el Sr. V. Bernardo, la Sra. C.-A. Marnier y los Sres. D. Nardi y M. Pollmann, en calidad de agentes;

– en nombre de la Agencia de la Unión Europea para la Ciberseguridad, por la Sra. A. Bourka, en calidad de agente;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 28 de septiembre de 2023;

dicta la siguiente

Sentencia

1 La petición de decisión prejudicial tiene por objeto la interpretación de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 2002, L 201, p. 37), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (DO 2009, L 337, p. 11) (en lo sucesivo, «Directiva 2002/58»), a la luz de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

2 Esta petición se ha presentado en el contexto de un litigio entre las asociaciones La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net y French Data Network, de una parte, y el Premier ministre (Primer Ministro, Francia) y el ministre de la Culture (Ministro de Cultura, Francia), de otra parte, en relación con la legalidad del décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » (Decreto n.º 2010-236, de 5 de marzo de 2010, relativo al tratamiento automatizado de datos personales autorizado por el artículo L. 331-29 del Código de la Propiedad Intelectual denominado «Sistema de gestión de medidas para la protección de las obras en Internet») (JORF n.º 56 de 7 de marzo de 2010, texto n.º 19), en su versión modificada por el décret nº 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (Decreto n.º 2017-924, de 6 de mayo de 2017, relativo a la gestión de los derechos de autor y de los derechos afines por un organismo de gestión de derechos y por el que se modifica el Código de la Propiedad Intelectual) (JORF n.º 109 de 10 de mayo de 2017, texto n.º 176) (en lo sucesivo, «Decreto n.º 2010-236»).

Marco jurídico

Derecho de la Unión

Normativa general sobre la protección de los datos personales

– *Directiva 95/46/CE*

3 Incluido en la sección II, que llevaba como título «Principios relativos a la legitimación del tratamiento de datos», del capítulo II de 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), el artículo 7 de esta Directiva tenía el siguiente tenor:

«Los Estados miembros dispondrán que el tratamiento de datos personales solo pueda efectuarse si:

[…]

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.»

4 El artículo 13, apartado 1, de dicha Directiva establecía:

«Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

[…]

g) la protección del interesado o de los derechos y libertades de otras personas.»

– *RGPD*

5 El artículo 2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO 2016, L 119, p. 1; en lo sucesivo, «RGPD»), titulado «Ámbito de aplicación material», dispone en sus apartados 1 y 2:

«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:

[…]

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.»

6 El artículo 4 del RGPD, titulado «Definiciones», dispone:

«A efectos del presente Reglamento se entenderá por:

1) “datos personales”: toda información sobre una persona física identificada o identificable (“el interesado”); […]

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;

[…]».

7 El artículo 6 de este Reglamento, titulado «Licitud del tratamiento», preceptúa lo siguiente en su apartado 1:

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

[…]

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales […].

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.»

8 El artículo 9 del citado Reglamento, que lleva como título «Tratamiento de categorías especiales de datos personales», establece, en su apartado 2, letras e) y f), que la prohibición del tratamiento de determinados tipos de datos personales que, entre otros, revele datos relativos a la vida sexual o la orientación sexual de una persona física no es de aplicación cuando el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos o es necesario para la formulación, el ejercicio o la defensa de reclamaciones.

9 El artículo 23 del RGPD, titulado «Limitaciones», dispone en su apartado 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:

[…]

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

j) la ejecución de demandas civiles.»

Normativa sectorial sobre la protección de los datos personales

– *Directiva 2002/58*

10 Los considerandos 2, 6, 7, 11, 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 comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, [hecho 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.

[…]

(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. […]

[…]

(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. […]»

11 A tenor del artículo 2 de la Directiva 2002/58, titulado «Definiciones»:

«[…]

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;

[…]».

12 El artículo 3 de esta Directiva, titulado «Servicios afectados», dispone:

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

13 A tenor del artículo 5 de dicha Directiva, titulado «Confidencialidad de las comunicaciones»:

«1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes

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

[…]

3. Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva [95/46]. […]»

14 El artículo 6 de la referida Directiva, titulado «Datos de tráfico», establece:

«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.»

15 El artículo 15 de la Directiva 2002/58, titulado «Aplicación de determinadas disposiciones de la Directiva [95/46]», presenta el siguiente tenor:

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

[…]

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

[…]»

– *Directiva (UE) 2016/680*

16 El artículo 1 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), que se titula «Objeto y objetivos», establece en su apartado 1:

«La presente Directiva establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.»

17 El artículo 3 de la referida Directiva, con el título «Definiciones», dispone:

«A efectos de la presente Directiva se entenderá por:

[…]

7) “autoridad competente”:

a) toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, o

b) cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública;

[…]».

Normativa sobre la protección de los derechos de propiedad intelectual

18 El artículo 8 de la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual (DO 2004, L 157, p. 45; corrección de errores en DO 2004, L 195, p. 16), titulado «Derecho de información», dispone:

«1. Los Estados miembros garantizarán que, en el contexto de los procedimientos relativos a una infracción de un derecho de propiedad intelectual y en respuesta a una petición justificada y proporcionada del demandante, las autoridades judiciales competentes puedan ordenar que faciliten datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen un derecho de propiedad intelectual el infractor […]:

[…]

2. Los datos a los que se refiere el apartado 1 incluirán, según proceda:

a) los nombres y direcciones de los productores, fabricantes, distribuidores, suministradores y otros poseedores anteriores de las mercancías o servicios, así como de los mayoristas y minoristas destinatarios;

[…]

3. Los apartados 1 y 2 se aplicarán sin perjuicio de otras disposiciones legales que:

a) concedan al titular derechos de información más amplios;

b) regulen la utilización de los datos que se comuniquen con arreglo al presente artículo en procedimientos civiles o penales;

c) regulen la responsabilidad por abuso del derecho de información;

d) ofrezcan la posibilidad de negarse a facilitar datos que obliguen a la persona a la que se refiere el apartado 1 a admitir su propia participación o la de sus parientes cercanos en una infracción de un derecho de propiedad intelectual,

o

e) rijan la protección de la confidencialidad de las fuentes de información o el tratamiento de los datos personales.»

Derecho francés

CPI

19 El artículo L. 331-12 del code de la propriété intellectuelle (Código de la Propiedad Intelectual), en su redacción vigente en la fecha de la resolución impugnada por las demandantes en el litigio principal (en lo sucesivo, «CPI»), dispone:

«La Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [(Alta Autoridad para la Difusión de Obras y la Protección de los Derechos en Internet, Francia) (en lo sucesivo, "Hadopi")] es una autoridad pública independiente. […]»

20 El artículo L. 331-13 de este Código establece:

«La [Hadopi] ejerce:

1.° la misión de promover el desarrollo de la oferta legal y de observar la utilización lícita e ilícita de las obras y objetos a los que estén ligados derechos de autor o derechos afines en las redes de comunicaciones electrónicas utilizadas para la prestación de servicios de comunicación al público en línea;

2.° la misión de proteger esas obras y objetos contra las infracciones de esos derechos cometidas en las redes de comunicaciones electrónicas utilizadas para la prestación de servicios de comunicación al público en línea;

[…]».

21 A tenor del artículo L. 331-15 del citado Código:

«La [Hadopi] se compone de un Colegio y una Comisión de Protección de los Derechos. […]

[…]

En el ejercicio de sus funciones, los miembros del Colegio y de la Comisión de Protección de los Derechos no recibirán instrucciones de ninguna autoridad.»

22 El artículo L. 331-17, párrafo primero, del referido Código dispone:

«La Comisión de Protección de los Derechos se encargará de adoptar las medidas previstas en el artículo L. 331-25.»

23 Con arreglo al artículo L. 331-21 del CPI:

«Para el ejercicio por la Comisión de Protección de los Derechos de sus atribuciones, la [Hadopi] dispondrá de agentes públicos jurados autorizados por [su] presidente en las condiciones establecidas mediante decreto adoptado previo dictamen del Conseil d'État [(Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia)]. […]

Los miembros de la Comisión de Protección de los Derechos y los agentes mencionados en el párrafo primero recibirán las denuncias dirigidas a dicha Comisión en las condiciones establecidas en el artículo L. 331-24 y procederán al examen de los hechos.

Para las necesidades del procedimiento, podrán obtener todos los documentos, cualquiera que sea su soporte, incluidos los datos conservados y procesados por los operadores de comunicaciones electrónicas en virtud del artículo L. 34-1 del code des postes et des communications électroniques [(Código de Correos y Comunicaciones Electrónicas)] y los prestadores de servicios mencionados en los puntos 1 y 2 del apartado I del artículo 6 de la loi nº 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)].

Asimismo, podrán obtener una copia de todos los documentos mencionados en el párrafo anterior.

En particular, podrán obtener de los operadores de comunicaciones electrónicas la identidad, la dirección postal, la dirección electrónica y los datos telefónicos del abonado cuyo acceso a los servicios de comunicación pública en línea haya sido utilizado con fines de reproducción, representación, puesta a disposición o comunicación al público de obras u objetos protegidos sin la autorización de los titulares de los derechos […], cuando se requiera tal autorización.»

24 El artículo L. 331-24 de este Código establece:

«La Comisión de Protección de los Derechos actúa en respuesta a las denuncias recibidas de los agentes jurados autorizados […] que son designados por:

– los organismos de defensa profesional debidamente constituidos;

– las entidades de gestión colectiva, y

– el Centre national du cinéma et de l'image animée [(Centro Nacional de Cine y Películas de Animación, Francia)].

La Comisión de Protección de los Derechos también podrá actuar sobre la base de la información que le transmita el fiscal de la República.

No podrán ponerse en conocimiento de la Comisión de Protección de los Derechos hechos cuya antigüedad sea superior a seis meses.»

25 En virtud del artículo L. 331-25 de dicho Código, que regula el denominado «procedimiento de respuesta gradual»:

«Cuando tenga conocimiento de hechos que puedan constituir un incumplimiento de la obligación prevista en el artículo L. 336-3 [del CPI], la Comisión de Protección de los Derechos podrá remitir al abonado […] una recomendación recordándole las disposiciones del artículo L. 336-3, instándole a respetar la obligación definida en las mismas y advirtiéndole de las sanciones previstas en los artículos L. 335-7 y L. 335-7-1. Esta recomendación incluirá asimismo información para el abonado sobre las ofertas legales de contenidos culturales en línea y sobre la existencia de medios de protección para evitar el incumplimiento de la obligación prevista en el artículo L. 336-3, así como sobre los peligros para la renovación de la creación artística y para la economía del sector cultural de las prácticas que no respetan los derechos de autor y los derechos afines.

En caso de que se repitan hechos que puedan constituir un incumplimiento de la obligación prevista en el artículo L. 336-3 en un plazo de seis meses a partir del envío de la recomendación a que se refiere el párrafo primero, la Comisión podrá remitir por vía electrónica una nueva recomendación que contenga la misma información que la anterior […]. Deberá acompañar dicha recomendación de

una carta enviada con acuse de recibo o cualquier otro medio que sirva para establecer la prueba de la fecha de presentación de esta recomendación.

Las recomendaciones emitidas en virtud del presente artículo mencionarán la fecha y la hora en que se constataron los hechos que puedan constituir un incumplimiento de la obligación prevista en el artículo L. 336-3. Sin embargo, no divulgarán el contenido de las obras u objetos protegidos afectados por dicho incumplimiento. En ellas se indicarán los datos telefónicos, postales y electrónicos donde el destinatario podrá, si así lo desea, presentar sus observaciones a la Comisión de Protección de los Derechos y obtener, si lo solicita expresamente, detalles sobre el contenido de las obras u objetos protegidos afectados por el incumplimiento que se le imputa.»

26 El artículo L. 331-29 del CPI establece:

«Se autoriza a la [Hadopi] a crear un sistema de tratamiento automatizado de datos personales relativos a las personas que son objeto de un procedimiento en el marco de la presente subsección.

La finalidad de este tratamiento será permitir a la Comisión de Protección de los Derechos ejecutar las medidas previstas en la presente subsección, todos los actos procesales relacionados y las modalidades de información de los organismos de defensa profesional y las entidades de gestión colectiva del eventual sometimiento de asuntos a la autoridad judicial, así como las notificaciones previstas en el párrafo quinto del artículo L. 335-7.

Mediante decreto […] se establecerán las normas de desarrollo del presente artículo. En particular, precisará:

– las categorías de datos recogidos y su período de conservación;

– los destinatarios facultados para recibir la comunicación de estos datos, en particular las personas cuya actividad consista en ofrecer acceso a servicios de comunicación al público en línea;

– las condiciones en las que las personas interesadas pueden ejercer, ante la [Hadopi], su derecho de acceso a los datos que les conciernen […]».

27 El artículo L. 335-2, párrafos primero y segundo, de dicho Código especifica:

«Toda edición de escritos, de composición musical, de dibujos, de pintura o de cualquier otra producción, impresa o grabada total o parcialmente, que no observe las leyes y reglamentos sobre la propiedad de los autores constituirá vulneración del derecho de propiedad intelectual y cualquier vulneración del derecho de propiedad intelectual constituye infracción penal.

La vulneración del derecho de propiedad intelectual en Francia de obras publicadas en Francia o en el extranjero se castigará con pena de prisión de tres años y multa de 300 000 euros».

28 El artículo L. 335-4, párrafo primero, de dicho Código indica:

«Se castigará con pena de prisión de tres años y multa de 300 000 euros cualquier fijación, reproducción, comunicación o puesta a disposición del público, a título oneroso o gratuito, o cualquier difusión televisiva de una prestación, de un fonograma, de un videograma, de un programa o de una publicación de prensa que se realice sin la autorización, cuando se requiera, del artista-intérprete, del productor de fonogramas o videogramas, de la empresa de comunicación audiovisual, del editor de prensa o de la agencia de prensa.»

29 El artículo L. 335-7 del CPI prescribe las reglas para la imposición a las personas culpables de las infracciones penales tipificadas en los artículos L. 335-2 y L. 335-4 de dicho Código de la pena accesoria de suspensión del acceso a un servicio de comunicación al público en línea durante un máximo de un año.

30 El artículo L. 335-7-1, párrafo primero, de dicho Código tiene el siguiente tenor:

«Para las infracciones penales de quinta clase (infracciones penales menores) que se contemplan en el presente Código, cuando el reglamento lo prevea, la pena accesoria definida en el artículo L. 335-7 podrá imponerse según el mismo régimen, en caso de negligencia grave, al titular del acceso a un servicio de comunicación al público en línea al que la Comisión de Protección de los Derechos, en aplicación del artículo L. 331-25, haya dirigido previamente, mediante carta enviada con acuse de recibo o cualquier otro medio que sirva para establecer la prueba de la fecha de presentación, una recomendación en que se le invite a implantar un medio de protección de su acceso a Internet.»

31 A tenor del artículo L. 336-3 del mencionado Código:

«El titular del acceso a servicios de comunicación al público en línea está obligado a velar por que este acceso no sea usado con fines de reproducción, representación, puesta a disposición o comunicación al público de obras u objetos protegidos por derechos de autor o derechos afines sin autorización de los titulares […], cuando se requiera tal autorización.

El incumplimiento de la obligación a que se refiere el párrafo primero por parte del titular del acceso no tiene por efecto que el interesado incurra en responsabilidad penal […]».

32 El artículo R. 331-37, párrafo primero, del CPI preceptúa:

«Los operadores de comunicaciones electrónicas […] y los proveedores […] están obligados a comunicar, mediante la interconexión con el tratamiento automatizado de datos personales mencionado en el artículo L. 331-29 o recurriendo a un soporte de grabación que garantice su integridad y seguridad, los datos personales y la información mencionada en el punto 2.° del anexo del Decreto [n.º 2010-236], en un plazo de ocho días contados a partir de la transmisión por la Comisión de Protección de los Derechos de los datos técnicos necesarios para la identificación del abonado cuyo acceso a datos de comunicación al público en línea se haya utilizado para la reproducción, representación, puesta a disposición o comunicación al público de obras u objetos protegidos sin autorización de los titulares de los derechos […], cuando se requiera tal autorización.»

33 De conformidad con el artículo L. 331-40 de dicho Código:

«Cuando, en el plazo de un año desde la presentación de la recomendación a que se refiere el párrafo primero del artículo L. 335-7-1, se pongan en conocimiento de la Comisión de Protección de Derechos nuevos hechos que puedan ser constitutivos de la negligencia grave tipificada en el artículo R. 335-5, esta informará al abonado, mediante carta enviada con acuse de recibo, de que esos hechos pueden dar lugar a acciones penales. En la carta se dará al interesado un plazo de quince días para presentar alegaciones; se señalará que, dentro del mismo plazo, podrá solicitar una audiencia al amparo del artículo L. 331-21-1 y que podrá estar asistido por un abogado. En la misma se le dará también la posibilidad de indicar sus cargas familiares y sus recursos económicos.

La Comisión podrá, de oficio, citar al interesado a una audiencia. En la carta de citación se indicará que tiene derecho a estar asistido por un abogado».

34 El artículo R. 335-5 del CPI establece:

«I.– Constituye negligencia grave, castigada con la multa prevista para las infracciones penales de quinta clase, el hecho de que el titular de un acceso a los servicios de comunicación al público en línea, sin una razón legítima, cuando se cumplan los requisitos establecidos en el apartado II:

1.° no haya establecido un medio de protección de dicho acceso, o

2.° haya actuado sin la diligencia debida en la implantación de este medio.

II.– Las disposiciones del apartado I solo serán aplicables cuando se cumplan los dos requisitos siguientes:

1.° de conformidad con el artículo L. 331-25 y en la forma prevista por dicho artículo, la Comisión de Protección de los Derechos ha recomendado al titular del acceso que implante un medio de protección de su acceso para evitar que vuelva a utilizarse con fines de reproducción, representación, puesta a disposición o comunicación al público de obras u objetos protegidos por derechos de autor o derechos afines sin autorización de los titulares de los derechos […], cuando se requiera tal autorización;

2.° en el plazo de un año a partir de la presentación de esta recomendación, dicho acceso se ha utilizado de nuevo para los fines mencionados en el punto 1.° del presente apartado II.»

35 A partir del 1 de enero de 2022, en aplicación de la loi n° 2021-1382, du 25 octobre 2021, relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique (Ley n.° 2021-1382, de 25 de octubre de 2021, de Regulación y Protección del Acceso a las Obras Culturales en la Era Digital) (JORF n.° 250, de 26 de octubre de 2021, texto n.° 2), se fusionó a la Hadopi con el Conseil supérieur de l'audiovisuel (CSA) (Consejo Superior de lo Audiovisual, Francia), otra autoridad pública independiente, para formar la Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) (Autoridad Reguladora de la Comunicación Audiovisual y Digital, Francia).

36 No obstante, el procedimiento de respuesta gradual a que se ha hecho referencia en el apartado 25 de la presente sentencia se mantuvo inalterado en lo esencial, si bien, ahora, no lo aplica la Comisión de Protección de Derechos de la Hadopi, que estaba integrada por tres miembros designados respectivamente por el Conseil d'État (Consejo de Estado), la Cour des comptes (Tribunal de Cuentas, Francia) y la Cour de cassation (Tribunal de Casación, Francia), sino por dos miembros del Colegio de la ARCOM, uno de los cuales lo designa el Conseil d'État (Consejo de Estado) y el otro la Cour de cassation (Tribunal de Casación).

Decreto n.° 2010-236

37 El Decreto n.° 2010-236, que se adoptó, en particular, sobre la base del artículo L. 331-29 del CPI, establece en su artículo 1:

«La finalidad del tratamiento de datos personales denominado "Sistema de gestión de medidas para la protección de las obras en Internet" es la ejecución por parte de la Comisión de Protección de los Derechos de la [Hadopi]:

1.° de las medidas previstas en el libro III de la parte legislativa del [CPI] (título III, capítulo I, sección 3, subsección 3) y en el libro III de la parte reglamentaria de dicho Código (título III, capítulo I, sección 2, subsección 2);

2.° de las denuncias transmitidas al fiscal de la República de los hechos que puedan constituir infracciones previstas en los artículos L. 335-2, L. 335-3, L. 335-4 y R. 335-5 del mismo Código, así como de la información relativa a estas denuncias a los organismos de defensa profesional y a las entidades de gestión colectiva;

[…]».

38 El artículo 4 de este Decreto preceptúa:

«I.– Los agentes públicos jurados autorizados por el presidente de la [Hadopi] en virtud del artículo L. 331-21 del [CPI] y los miembros de la Comisión de Protección de los Derechos mencionada en el artículo 1 tendrán acceso directo a los datos personales y a la información a que se refiere el anexo del presente Decreto.

II.– Los operadores de comunicaciones electrónicas y los prestatarios mencionados en el punto 2.° del anexo del presente Decreto serán destinatarios:

– de los datos técnicos necesarios para la identificación del abonado;

– de las recomendaciones previstas en el artículo L. 331-25 del [CPI] con el fin de enviarlas por vía electrónica a sus abonados;

– de los elementos necesarios para la aplicación de las sanciones accesorias de suspensión del acceso a un servicio de comunicación al público en línea puestas en conocimiento de la Comisión de Protección de los Derechos por el fiscal de la República.

III.– Los organismos de defensa profesional y las entidades de gestión colectiva serán destinatarias de la información relativa a la transmisión de la denuncia al fiscal de la República.

IV.– Las autoridades judiciales serán destinatarias de las actas de comprobación de hechos que puedan constituir infracciones previstas en los artículos L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 y R. 335-5 del [CPI].

Se incluirá en el registro de antecedentes penales automatizado información sobre la ejecución de la pena de suspensión.»

39 El anexo de dicho Decreto dispone:

«Los datos personales y la información registrados en el sistema de tratamiento denominado "Sistema de gestión de medidas para la protección de las obras en Internet" son los siguientes:

1.° Datos personales e información procedente de los organismos de defensa profesional debidamente constituidos, de las entidades de gestión colectiva, del Centro Nacional de Cine y Películas de Animación y del fiscal de la República:

Por lo que se refiere a los hechos que puedan constituir un incumplimiento de la obligación prevista en el artículo L. 336-3 del [CPI]:

fecha y hora de los hechos;

dirección IP de los abonados afectados;

protocolo entre pares ("peer-to-peer") utilizado;

seudónimo utilizado por el abonado;

información sobre las obras u objetos protegidos afectados por los hechos;

nombre del archivo tal y como se encuentra en la estación del abonado (si procede), y

el proveedor de servicios de Internet con el que se contrató el acceso o que proporcionó el recurso técnico IP.

[…]

2.° Los datos personales y la información sobre los abonados obtenidos de los operadores de comunicaciones electrónicas […] y los proveedores […]:

nombre y apellido;

dirección postal y direcciones electrónicas;

datos telefónicos;

dirección de la instalación de la línea telefónica del abonado;

proveedor de servicios de Internet, que utiliza los recursos técnicos del proveedor de servicios mencionado en el punto 1.°, con el que el abonado ha celebrado un contrato; número de expediente;

fecha de inicio de la suspensión del acceso a un servicio de comunicación al público en línea.

[…]»

Código de Correos y Comunicaciones Electrónicas

40 El artículo L. 34-1, II *bis*, del Código de Correos y Comunicaciones Electrónicas dispone:

«Los operadores de comunicaciones electrónicas están obligados a conservar:

1.° a efectos de los procesos penales, de la prevención de amenazas contra la seguridad pública y de la salvaguardia de la seguridad nacional, la información relativa a la identidad civil del usuario hasta la expiración de un plazo de cinco años a partir del fin de la validez de su contrato;

2.° para los mismos fines enunciados en el punto 1.° del presente apartado II *bis*, cualquier otra información facilitada por el usuario en el momento de la celebración de un contrato o de la creación de una cuenta, así como la información relativa al pago, hasta la expiración de un plazo de un año a partir del fin de la validez de su contrato o de la cancelación de su cuenta;

3.° a efectos de la lucha contra la criminalidad y la delincuencia grave, de la prevención de amenazas graves contra la seguridad pública y de la salvaguardia de la seguridad nacional, los datos técnicos que permitan identificar el origen de la conexión o los relativos a los equipos terminales utilizados, hasta la expiración de un plazo de un año a partir de la conexión o utilización de los equipos terminales.»

Litigio principal y cuestiones prejudiciales

41 Al haber desestimado tácitamente el Primer Ministro la solicitud que habían presentado con el objeto de que se derogase el Decreto n.º 2010-236, las demandantes en el litigio principal interpusieron ante el Conseil d'État (Consejo de Estado), el 12 de agosto de 2019, recurso de anulación contra tal resolución de desestimación tácita. Alegaron, en esencia, que el artículo L. 331-21, párrafos tercero a quinto, del CPI, que forma parte de la base legal de dicho Decreto, por un lado, contraviene el derecho al respeto de la vida privada consagrado en la Constitución francesa y, por otro lado, viola el Derecho de la Unión, en particular el artículo 15 de la Directiva 2002/58 y los artículos 7, 8, 11 y 52 de la Carta.

42 Por lo que se refiere al aspecto del recurso relativo a la supuesta violación de la Constitución, el Conseil d'État (Consejo de Estado) planteó al Conseil constitutionnel (Consejo Constitucional, Francia) una cuestión prioritaria de constitucionalidad.

43 Mediante la resolución n.º 2020-841 QPC de 20 de mayo de 2020, La Quadrature du Net y otros [Derecho de comunicación a la Hadopi], el Conseil constitutionnel (Consejo Constitucional) declaró contrarios a la Constitución los párrafos tercero y cuarto del artículo L. 331-21 del CPI, pero declaró conforme con ella el párrafo quinto de dicho artículo, con excepción de los términos «en particular».

44 Por lo que atañe al aspecto del recurso relativo a la supuesta violación del Derecho de la Unión, las demandantes en el litigio principal sostuvieron, en concreto, que el Decreto n.º 2010-236 y las disposiciones que conforman su base legal autorizan el acceso a datos de conexión de manera desproporcionada por infracciones de los derechos de autor cometidas en Internet que no son graves, sin control previo de un juez o de una autoridad que ofrezca garantías de independencia e

imparcialidad. Entienden, concretamente, que estas infracciones no están comprendidas en la «delincuencia grave» a la que se refiere la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970).

45 A este respecto, el Conseil d'État (Consejo de Estado) recuerda, por una parte, que, en la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), el Tribunal de Justicia declaró, en particular, que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a medidas legislativas que 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. El Conseil d'État (Consejo de Estado) indica así que, en lo tocante a los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, es posible tal conservación, sin plazo concreto, con fines de investigación, detección y persecución de infracciones penales en general; la Directiva 2002/58 tampoco se opone a un acceso a esos datos con tales fines.

46 El órgano jurisdiccional remitente deduce de ello que, por lo que respecta al acceso a datos de identidad civil de los usuarios de medios de comunicaciones electrónicas, debe desestimarse el motivo de las demandantes en el litigio principal fundado en que el Decreto n.º 2010-236 es ilegal por haberse adoptado en el marco de la lucha contra infracciones que no son graves.

47 Por otra parte, dicho órgano jurisdiccional recuerda que, mediante la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), el Tribunal de Justicia declaró, en particular, que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin someter dicho acceso a un control previo por un órgano jurisdiccional o una entidad administrativa independiente.

48 El órgano jurisdiccional remitente hace referencia, más concretamente, al apartado 120 de dicha sentencia, en el que el Tribunal de Justicia precisó que es esencial que tal acceso a los datos conservados esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se produzca a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, descubrimiento o acciones penales.

49 El órgano jurisdiccional remitente señala que el Tribunal de Justicia recordó esta exigencia en la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), a propósito de la recopilación en tiempo real de los datos de conexión por los servicios de inteligencia, y en la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, EU:C:2021:152), en lo referente al acceso de las autoridades nacionales a los datos de conexión.

50 El órgano jurisdiccional remitente observa asimismo que, desde que se creara en 2009, la Hadopi ha remitido más de 12,7 millones de recomendaciones a titulares de abonos en el marco del denominado «procedimiento de respuesta gradual» del artículo L. 331-25 del CPI, 827 791 de las cuales se remitieron tan solo en 2019. Ello supone que los agentes de la Comisión de Protección de

los Derechos de la Hadopi han tenido necesariamente que recoger, cada año, una cantidad considerable de datos de identidad civil de los usuarios de que se trata. Dicho órgano jurisdiccional entiende que, dado el volumen de esas recomendaciones, someter esa recogida a control previo podría hacer imposible aplicar dichas recomendaciones.

51 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) ¿Los datos de identidad civil correspondientes a una dirección IP se encuentran entre los datos de tráfico o de localización sujetos, en principio, a la obligación de control previo por un órgano jurisdiccional o una entidad administrativa independiente con poder vinculante?

2) En caso de respuesta afirmativa a la primera cuestión prejudicial, a la vista de la escasa sensibilidad de los datos relativos a la identidad civil de los usuarios, incluidos sus datos de contacto, ¿debe interpretarse la Directiva [2002/58], a la luz de la [Carta], en el sentido de que se opone a una normativa nacional que prevé la recogida de estos datos correspondientes a la dirección IP de usuarios por una autoridad administrativa, sin control previo por un órgano jurisdiccional o una entidad administrativa independiente con poder vinculante?

3) En caso de respuesta afirmativa a la segunda cuestión prejudicial, y a la vista de la escasa sensibilidad de los datos relativos a la identidad civil, de la circunstancia de que solo puedan recogerse estos datos para las necesidades de la prevención de incumplimientos de obligaciones definidas de forma precisa, limitada y restrictiva por el Derecho nacional y de la circunstancia de que un control sistemático del acceso a los datos de cada usuario por un órgano jurisdiccional o una tercera entidad administrativa dotada de poder vinculante podría poner en peligro el cumplimiento de la misión de servicio público conferida a la propia autoridad administrativa independiente que procede a esta recogida de datos, ¿se opone la Directiva [2002/58] a que este control se efectúe conforme a modalidades adaptadas, tales como un control automatizado, en su caso bajo la supervisión de un servicio interno del organismo que ofrezca garantías de independencia e imparcialidad en relación con los agentes encargados de realizar esta recogida?»

Sobre las cuestiones prejudiciales

52 Mediante sus tres cuestiones prejudiciales, que procede examinar conjuntamente, el órgano jurisdiccional remitente pregunta, en esencia, si el artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que autoriza a la autoridad pública encargada de proteger los derechos de autor y los derechos afines a los derechos de autor contra las vulneraciones de esos derechos cometidas en Internet a acceder a los datos, conservados por los proveedores de servicios de comunicaciones electrónicas accesibles para el público, de identidad civil correspondientes a direcciones IP recabadas previamente por organizaciones de titulares de derechos, con el propósito de que dicha autoridad pública pueda identificar a los titulares de esas direcciones, utilizadas para actividades que pudieran ser constitutivas de tales vulneraciones, y, en su caso, pueda adoptar medidas contra ellos, sin que ese acceso se condicione al control previo de un órgano jurisdiccional o de una entidad administrativa independiente.

Observaciones preliminares

53 Son objeto de controversia en el litigio principal dos tratamientos de datos personales distintos y sucesivos que se producen en el marco de las actividades de la Hadopi, autoridad pública independiente que tiene como misión, en particular, con arreglo al artículo L. 331-13 del CPI, proteger las obras y objetos protegidos por derechos de autor o derechos afines a los derechos de autor contra las vulneraciones de esos derechos que se cometan en las redes de comunicaciones electrónicas utilizadas para la prestación de servicios de comunicación al público en línea.

54 El primer tratamiento, efectuado por agentes jurados autorizados de las organizaciones de titulares de derechos, consta de dos fases. En la primera de ellas, las direcciones IP que parezcan haberse utilizado para actividades que pudieran ser constitutivas de vulneración del derecho de autor o de un derecho afín a los derechos de autor se recogen en las redes entre pares (*peer-to-peer*). En la segunda fase, se pone a disposición de la Hadopi, en actas, un conjunto de datos personales y de información. Se trata, según la lista que figura en el punto 1.° del anexo del Decreto 2010/236, de la fecha y la hora de los hechos, la dirección IP de los abonados en cuestión, el protocolo entre pares usado, el seudónimo utilizado por el abonado, la información sobre las obras u objetos protegidos afectados por los hechos, el nombre del archivo tal y como se encuentra en la estación del abonado (si procede) y el proveedor de servicios de Internet con el que se contrató el acceso o que proporcionó el recurso técnico IP.

55 El segundo tratamiento, efectuado por los proveedores de acceso a Internet a requerimiento de la Hadopi, también consta de dos fases. En la primera de ellas, las direcciones IP previamente recabadas se asocian a los titulares de esas direcciones. En la segunda fase, se pone a disposición de esa autoridad pública un conjunto de información y datos personales de dichos titulares esencialmente referidos a su identidad civil. Se trata fundamentalmente, según la lista que figura en el punto 2.° del anexo del Decreto n.º 2010-236, del nombre y apellido, la dirección postal y las direcciones electrónicas, los datos telefónicos y la dirección de la instalación de la línea telefónica del abonado.

56 A este último respecto, el artículo L. 331-21 del CPI establece, en su párrafo quinto, en la versión resultante de la resolución del Conseil constitutionnel (Consejo Constitucional) a que se ha hecho referencia en el apartado 43 de la presente sentencia, que los miembros de la Comisión de Protección de los Derechos de la Hadopi y los agentes públicos jurados de esta autoridad autorizados por su presidente pueden requerir a los operadores de comunicaciones electrónicas para que les faciliten la identidad, la dirección postal, la dirección electrónica y los datos telefónicos del abonado cuyo acceso a los servicios de comunicación pública en línea se haya utilizado con fines de reproducción, representación, puesta a disposición o comunicación al público de obras u objetos protegidos sin la autorización de los titulares de los derechos, cuando se requiera tal autorización.

57 Estos distintos tratamientos de datos personales tienen como finalidad que la Hadopi pueda adoptar, frente a los titulares de direcciones IP a los que se haya identificado de esta manera, las medidas previstas en el marco del denominado procedimiento administrativo de respuesta gradual del artículo L. 331-25 del CPI. Esas medidas son, primero, el envío de «recomendaciones», que se asemejan a advertencias; segundo, en caso de que se someta el asunto a la Comisión de Derechos de la Hadopi, en el plazo de un año desde el envío de una segunda recomendación, por hechos que pudieran constituir reiteración del incumplimiento constatado, la información dirigida al abonado, a la que se refiere el artículo R. 331-40 del CPI, según la cual los hechos pueden ser constitutivos de la denominada infracción penal menor de «negligencia

grave», tipificada en el artículo R. 335-5 del CPI y que se castiga con multa de hasta 1 500 euros y, en caso de reincidencia, con multa de hasta 3 000 euros, y tercero, tras deliberación, la denuncia al Ministerio Fiscal de hechos que pudieran ser constitutivos de tal infracción penal menor o, en su caso, de la infracción penal de vulneración del derecho de propiedad intelectual que se tipifica en el artículo L. 335-2 del CPI o en el artículo L. 335-4 del mismo y que se castiga con pena de prisión de tres años y multa de 300 000 euros.

58 Precisado lo anterior, las cuestiones prejudiciales que plantea el órgano jurisdiccional remitente solo se refieren al segundo tratamiento, descrito en el apartado 55 de la presente sentencia, y no al primero, cuyas principales características se han expuesto en el apartado 54 de la misma.

59 No obstante, ha de señalarse que, si la recogida previa, por parte de las organizaciones de titulares de derechos, de las direcciones IP contraviniera el Derecho de la Unión, este se opondría igualmente a la explotación de esos datos en el marco del posterior tratamiento efectuado por los proveedores de servicios de comunicaciones electrónicas, que consiste en asociar esas direcciones a los datos de identidad civil de los titulares de dichas direcciones.

60 En este contexto, ha de recordarse, de entrada, que, según la jurisprudencia del Tribunal de Justicia, las direcciones IP son tanto datos de tráfico a efectos de la Directiva 2002/58 como datos personales a efectos del RGPD (véase, en este sentido, la sentencia de 17 de junio de 2021, M.I.C.M., C-597/19, EU:C:2021:492, apartados 102 y 113 y jurisprudencia citada).

61 No obstante, la recogida de direcciones IP, públicas y visibles por todos, realizada por agentes de organizaciones de titulares de derechos, no está comprendida en el ámbito de aplicación de la Directiva 2002/58, pues tal tratamiento no se produce manifiestamente «en relación con la prestación de servicios de comunicaciones electrónicas», en el sentido del artículo 3 de esta Directiva.

62 En cambio, tal recogida de direcciones IP, que, como se desprende de los autos que obran en poder del Tribunal de Justicia, está sujeta, dentro de ciertos límites cuantitativos y con ciertas condiciones, a la autorización de la Commission nationale de l'informatique et des libertés (CNIL) (Comisión Nacional de Informática y de Libertades, Francia), para su transmisión a la Hadopi a los fines de su eventual utilización en posteriores procedimientos administrativos o judiciales con objeto de luchar contra las actividades que vulneren los derechos de autor y los derechos afines a los derechos de autor, constituye «tratamiento», en el sentido del artículo 4, punto 2, del RGPD, cuya licitud depende de los requisitos que prescribe el artículo 6, apartado 1, párrafo primero, letra f), de este Reglamento, a la luz de la jurisprudencia del Tribunal de Justicia derivada de las sentencias de 17 de junio de 2021, M.I.C.M. (C-597/19, EU:C:2021:492), apartados 102 y 103, y de 4 de julio de 2023, Meta Platforms y otros (Condiciones generales del servicio de una red social) (C-252/21, EU:C:2023:537), apartados 106 a 112 y jurisprudencia citada.

63 En cuanto al segundo tratamiento, descrito en el apartado 55 de la presente sentencia, entra en el ámbito de aplicación de la Directiva 2002/58 porque se produce «en relación con la prestación de servicios de comunicaciones electrónicas», en el sentido del artículo 3 de esta Directiva, pues los datos en cuestión se obtienen de los proveedores de servicios de comunicaciones electrónicas con arreglo al artículo L. 331-21 del CPI.

Sobre la existencia de justificación, con arreglo al artículo 15, apartado 1, de la Directiva 2002/58, del acceso de una autoridad pública a datos de identidad civil correspondientes a una dirección IP conservados por los proveedores de servicios de comunicaciones

electrónicas con el propósito de luchar contra la vulneración del derecho de propiedad intelectual cometida en línea

64 En vista de las anteriores observaciones preliminares, se plantea la cuestión de si, como se pregunta el órgano jurisdiccional remitente, la limitación de los derechos fundamentales consagrados en los artículos 7, 8 y 11 de la Carta que supone el acceso de una autoridad pública, como la Hadopi, a datos de identidad civil correspondientes a una dirección IP de la que esta autoridad ya dispone puede justificarse sobre la base del artículo 15, apartado 1, de la Directiva 2002/58.

65 Pues bien, el acceso a tales datos personales solo puede concederse a condición de que se hayan conservado de conformidad con la Directiva 2002/58 [véase, en este sentido, la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 29].

Sobre las exigencias aplicables a la conservación de los datos de identidad civil y de las direcciones IP correspondientes a estos datos por parte de los proveedores de servicios de comunicaciones electrónicas

66 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 de la utilización no autorizada del sistema de comunicaciones electrónicas. Para ello, los Estados miembros pueden adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por uno de esos motivos. 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 (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 110 y 111).

67 Por lo tanto, una medida legislativa adoptada en virtud de esta disposición debe responder efectiva y estrictamente a alguno de los objetivos mencionados en el apartado anterior, pues la enumeración de estos objetivos en el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 tiene carácter exhaustivo, y debe respetar los principios generales del Derecho de la Unión, entre los que figura el principio de proporcionalidad, así como los derechos fundamentales garantizados en 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 (véase, en este sentido, la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 112 y 113).

68 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 (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 114 y jurisprudencia citada).

69 A este respecto, ha de subrayarse que la conservación de los datos de tráfico y de los datos de localización constituye, de por sí, por un lado, una excepción a la prohibición, que se establece en el artículo 5, apartado 1, de la Directiva 2002/58, a cualquier persona que no sea el usuario de almacenar esos datos y, por otro lado, una injerencia en los derechos fundamentales al respeto a la vida privada y a la protección de los datos personales, consagrados en los artículos 7 y 8 de la Carta, sin que haya de determinarse si la información relativa a la vida privada de que se trate tiene o no carácter sensible o si los interesados han sufrido o no inconvenientes por esa injerencia. Es asimismo irrelevante que los datos conservados se utilicen o no posteriormente, 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 (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 115 y 116).

70 Ahora bien, en tanto en cuanto permite a los Estados miembros introducir determinadas medidas que establezcan excepciones, como se ha recordado en el apartado 66 de la presente sentencia, el artículo 15, apartado 1, de la Directiva 2002/58 refleja el hecho de que los derechos consagrados en los artículos 7, 8 y 11 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse de acuerdo con su función en la sociedad. En efecto, como se desprende del artículo 52, apartado 1, de la Carta, esta admite limitaciones del ejercicio de estos derechos, siempre que 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 (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 120 y 121).

71 En el caso de autos, ha de señalarse que, si bien, formalmente, la Hadopi está autorizada a acceder solo a los datos de identidad civil correspondientes a una dirección IP, ese acceso presenta la particularidad de que requiere, previamente, que los proveedores de servicios de comunicaciones electrónicas de que se trate asocien la dirección IP a los datos de identidad civil de su titular. Por tanto, dicho acceso presupone necesariamente que los proveedores dispongan de las direcciones IP y de los datos de identidad de sus titulares.

72 Además, esta autoridad pública pretende que se le conceda acceso a esos datos con el solo propósito de identificar al titular de una dirección IP que se haya utilizado para actividades que pudieran vulnerar los derechos de autor o los derechos afines a los derechos de autor, por haber puesto ilegalmente a disposición en Internet obras protegidas para que otras personas las descarguen. En estas circunstancias, debe considerarse que los datos de identidad civil están estrechamente ligados tanto a la dirección IP como a la información sobre la obra puesta a disposición en Internet de que la Hadopi dispone.

73 Pues bien, no puede hacerse caso omiso de tal contexto particular al examinar la eventual justificación de una medida de conservación de datos personales sobre la base del artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7, 8 y 11 de la Carta (véase, por analogía, Tribunal Europeo de Derechos Humanos [TEDH], sentencia de 24 de abril de 2018, Benedik c. Eslovenia, CE:ECHR:2018:0424JUD006235714, § 109).

74 Por lo tanto, la eventual justificación de la injerencia en los derechos fundamentales consagrados en los artículos 7, 8 y 11 de la Carta que supone la conservación, por parte de los proveedores de servicios de comunicaciones electrónicas accesibles para el público, de los datos a los que la Hadopi está autorizada a acceder tiene que examinarse a la luz de las exigencias que, en materia de conservación de direcciones IP, se derivan del artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los referidos artículos de la Carta.

75 En este contexto, se ha de subrayar que, según la jurisprudencia del Tribunal de Justicia, si bien, como se ha recordado en el apartado 60 de la presente sentencia, las direcciones IP constituyen datos de tráfico a efectos de la Directiva 2002/58, estas direcciones se distinguen de las demás categorías de datos de tráfico y de los datos de localización.

76 A este respecto, el Tribunal de Justicia ha señalado que las direcciones IP se generan sin estar vinculadas a una comunicación determinada y sirven fundamentalmente para identificar, por medio de los proveedores de servicios de comunicaciones electrónicas, al propietario 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 dio origen a la comunicación. En esta medida, esta categoría de datos presenta un grado de sensibilidad menor que los demás datos de tráfico (véase, en este sentido, la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 152).

77 Es cierto que, en el apartado 156 de la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), el Tribunal de Justicia declaró que, pese a apreciarse que las direcciones IP tienen menor sensibilidad cuando solo sirven para identificar al usuario de un servicio de comunicaciones electrónicas, el artículo 15, apartado 1, de la Directiva 2002/58 se opone a que una conservación generalizada e indiferenciada solo de las direcciones IP atribuidas al origen de una conexión se lleve a cabo para objetivos distintos de la lucha contra la delincuencia grave, la prevención de las amenazas graves contra la seguridad pública o la protección de la seguridad nacional. No obstante, para llegar a esa conclusión, el Tribunal de Justicia se basó expresamente en el carácter grave de la injerencia en los derechos fundamentales consagrados en los artículos 7, 8 y 11 de la Carta que puede suponer tal conservación de las direcciones IP.

78 En efecto, el Tribunal de Justicia consideró, en el apartado 153 de la referida sentencia, que, en la medida en que las direcciones IP, en particular cuando se utilizan para llevar a cabo el «rastreo exhaustivo de la secuencia de navegación de un internauta» y, en consecuencia, de su actividad en línea, pueden permitir establecer el «perfil detallado» de ese internauta, la conservación y el análisis de dichas direcciones IP que precisa tal rastreo constituyen injerencias graves en los derechos fundamentales de la persona afectada consagrados en los artículos 7 y 8 de la Carta, que también pueden tener efectos disuasorios en el ejercicio, por los usuarios de los medios de comunicación electrónicos, de su libertad de expresión garantizada en el artículo 11 de la Carta.

79 No obstante, ha de subrayarse que no toda conservación generalizada e indiferenciada de un conjunto, en su caso vasto, de direcciones IP estáticas y dinámicas que una persona haya utilizado en un determinado período constituye necesariamente una injerencia grave en los derechos fundamentales garantizados en los artículos 7, 8 y 11 de la Carta.

80 A este respecto, para empezar, los asuntos en que recayó la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), versaban sobre normativas nacionales que implicaban la obligación de conservar un conjunto de datos necesarios para 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 cuales figuraban, en particular, el nombre y la dirección del usuario, los números de teléfono de quien realizaba la llamada y de quien la recibía y la dirección IP para los servicios de Internet. Además, en dos de esos asuntos, las normativas nacionales en cuestión parecían abarcar asimismo los datos relativos a la conducción de las comunicaciones electrónicas por las redes, que permiten asimismo identificar la naturaleza de la información consultada en línea (véase, en este sentido, la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 82 y 83).

81 Así pues, la conservación de las direcciones IP realizada en el marco de tales normativas nacionales, habida cuenta de los demás datos a cuya conservación obligaban esas normativas y de la posibilidad de asociar esos distintos datos, hacía posible que se extrajeran conclusiones precisas sobre la vida privada de las personas de cuyos datos se trataba y, por tanto, que se produjera una injerencia grave en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, referentes a la protección de la vida privada y de los datos personales de esas personas, y en el artículo 11 de la misma, atinente a la libertad de expresión de dichas personas.

82 En cambio, la obligación impuesta a los proveedores de servicios de comunicaciones electrónicas, mediante una medida legislativa fundada en el artículo 15, apartado 1, de la Directiva 2002/58, de garantizar la conservación generalizada e indiferenciada de las direcciones IP puede en su caso estar justificada por el objetivo de luchar contra las infracciones penales en general cuando se excluye, de manera efectiva, que esa conservación pueda generar injerencias graves en la vida privada de la persona afectada debido a la posibilidad de extraer conclusiones precisas sobre ella, en particular asociando esas direcciones IP a un conjunto de datos de tráfico o de localización que también hayan conservado esos proveedores.

83 Consiguientemente, un Estado miembro que pretenda imponer a los proveedores de servicios de comunicaciones electrónicas la obligación de conservación generalizada e indiferenciada de las direcciones IP para alcanzar un objetivo ligado a la lucha contra las infracciones penales en general debe cerciorarse de que las condiciones de conservación de esos datos permitirán garantizar que se excluya que dichas direcciones IP se asocien a otros datos conservados, dentro del respeto de la Directiva 2002/58, de manera que pudieran extraerse conclusiones precisas sobre la vida privada de las personas cuyos datos se conserven de ese modo.

84 Para garantizar que se excluya que los datos se asocien de una manera tal que puedan extraerse conclusiones precisas sobre la vida privada de la persona de que se trate, las condiciones de conservación deben atañer a la propia estructura de la conservación, que, en esencia, debe organizarse de modo que se asegure una separación en compartimentos estancos de las diferentes categorías de datos conservados.

85 A este respecto, corresponde ciertamente al Estado miembro que pretenda imponer a los proveedores de servicios de comunicaciones electrónicas la obligación de conservación generalizada e indiferenciada de las direcciones IP para alcanzar un objetivo ligado a la lucha contra las infracciones penales en general establecer, en su legislación, normas claras y precisas sobre esas condiciones de conservación, condiciones que deben ajustarse a exigencias estrictas. No obstante, el Tribunal de Justicia puede dar detalles sobre esas condiciones.

86 Primero, las normas nacionales mencionadas en el apartado anterior deben garantizar que cada categoría de datos, incluidos los datos identidad civil y las direcciones IP, se conserve de forma totalmente separada de las demás categorías de datos conservados.

87 Segundo, esas normas deben garantizar que, en el plano técnico, la separación de las diferentes categorías de datos conservados, en particular los datos de identidad civil, las direcciones IP, los diferentes datos de tráfico que no sean direcciones IP y los distintos datos de localización, se haga en compartimentos estancos, con un sistema informático seguro y fiable.

88 Tercero, en caso de que dichas normas prevean la posibilidad de asociar las direcciones IP conservadas a la identidad civil de la persona de que se trate con observancia de las exigencias dimanantes del artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7, 8 y 11 de la Carta, solo deben permitir tal asociación mediante la utilización de un procedimiento técnico efectivo que no arroje dudas sobre la eficacia de la separación en compartimentos estancos de esas categorías de datos.

89 Cuarto, la fiabilidad de esa separación en compartimentos estancos debe someterse al control periódico de una autoridad pública distinta de la que pretende que se le conceda acceso a los datos personales conservados por los proveedores de servicios de comunicaciones electrónicas.

90 Siempre y cuando en la legislación nacional aplicable se establezcan tales exigencias estrictas para las condiciones de conservación generalizada e indiferenciada de las direcciones IP y de los demás datos conservados por los proveedores de servicios de comunicaciones electrónicas, la injerencia resultante de esa conservación de las direcciones IP no puede, debido a la propia estructura de dicha conservación, calificarse de «grave».

91 En efecto, en el caso de que se establezca un régimen legal de tales características, las condiciones de conservación de las direcciones IP fijadas de esta manera excluyen que esos datos puedan asociarse a otros datos conservados sobre la base de la Directiva 2002/58 de forma que sea posible extraer conclusiones precisas sobre la vida privada de la persona de que se trate.

92 Consiguientemente, de existir un régimen legal conforme con las exigencias expuestas en los apartados 86 a 89 de la presente sentencia, que garantice que ninguna asociación de datos permitirá extraer conclusiones precisas sobre la vida privada de la persona de que se trate, el artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7, 8 y 11 de la Carta, no se opone a que el Estado miembro de que se trate imponga la obligación de conservación generalizada e indiferenciada de las direcciones IP en pro del objetivo de lucha contra las infracciones penales en general.

93 Por último, como se desprende del apartado 168 de la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), tal régimen legal debe disponer un período de conservación limitado a lo estrictamente necesario y garantizar, con normas claras y precisas, que la conservación de los datos en cuestión se supedite al cumplimiento

de los correspondientes requisitos materiales y procedimentales y que las personas afectadas dispongan de garantías efectivas contra los riesgos de abuso y contra cualquier acceso y uso ilícitos de esos datos.

94 Corresponde al órgano jurisdiccional remitente comprobar si la normativa nacional controvertida en el procedimiento principal cumple las exigencias expuestas en los apartados 85 a 93 de la presente sentencia.

Sobre las exigencias para el acceso a los datos de identidad civil correspondientes a una dirección IP que conserven los proveedores de servicios de comunicaciones electrónicas

95 De la jurisprudencia del Tribunal de Justicia se desprende que, en el ámbito de la lucha contra las infracciones penales, solo los objetivos de lucha contra la delincuencia grave o de prevención de las amenazas graves contra la seguridad pública pueden justificar la injerencia grave en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que supone el acceso de las autoridades públicas a un conjunto de datos de tráfico o de datos localización, que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y que permiten extraer conclusiones precisas sobre la vida privada de las personas afectadas, sin que otros factores relativos a la proporcionalidad de la solicitud de acceso, como la duración del período para el que se solicita el acceso a tales datos, puedan conllevar que el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general justifique tal acceso [sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 35].

96 En cambio, cuando la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que supone el acceso de las autoridades públicas a los datos de identidad civil conservados por los proveedores de servicios de comunicaciones electrónicas, sin que esos datos puedan asociarse a la información relativa a las comunicaciones efectuadas, no es grave por cuanto, considerados en su conjunto, esos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados, dicho acceso puede estar justificado por un objetivo de prevención, investigación, descubrimiento y persecución de infracciones penales en general (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartados 54, 57 y 60).

97 Asimismo, es preciso añadir que, según un principio consagrado en reiterada jurisprudencia del Tribunal de Justicia, el acceso a datos de tráfico y a datos de localización solamente puede justificarse en virtud del artículo 15, apartado 1, de la Directiva 2002/58 por el objetivo de interés general para el que se haya impuesto su conservación a los proveedores de servicios de comunicaciones electrónicas, a menos que dicho acceso se justifique por un objetivo de interés general de mayor importancia. Se deduce concretamente de ese principio que tal acceso con fines de lucha contra las infracciones penales en general no puede concederse en ningún caso cuando la conservación de esos datos se haya justificado por el objetivo de lucha contra la delincuencia grave o, *a fortiori*, de protección de la seguridad nacional (véase, en este sentido, la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 166).

98 En cambio, tal objetivo de lucha contra las infracciones penales en general permite justificar que se dé acceso a los datos de tráfico y de localización que se hayan almacenado y por tanto conservado en la medida y por la duración necesarias para la comercialización de servicios, la facturación y la

prestación de servicios de valor añadido, como autoriza el artículo 6 de la Directiva 2002/58 (véase, en este sentido, la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 108 y 167).

99 En el presente asunto, en primer lugar, de la normativa nacional controvertida en el litigio principal se desprende que la Hadopi no tiene acceso a un «conjunto de datos de tráfico o de datos de localización», en el sentido de la jurisprudencia recordada en el apartado 95 de la presente sentencia, de modo que, en principio, no puede extraer conclusiones precisas sobre la vida privada de las personas de que se trate. Pues bien, un acceso que no permite extraer conclusiones de tal índole no constituye injerencia grave en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta.

100 En efecto, según la referida normativa y las explicaciones del Gobierno francés al respecto, el acceso que se concede a esa autoridad pública se limita estrictamente a determinados datos de identidad civil del titular de una dirección IP y se autoriza con el solo propósito de poder identificar a ese titular sobre el que hay sospechas de que ha realizado una actividad que vulnera los derechos de autor o los derechos afines a los derechos de autor, por haber puesto ilegalmente a disposición en Internet obras protegidas para que otras personas las descarguen. Ese acceso tiene como finalidad que, en su caso, se adopte frente a dicho titular alguna de las medidas pedagógicas o sancionadoras contempladas en el marco del procedimiento de respuesta gradual, esto es, el envío de una primera y de una segunda recomendación, seguida de una carta en que se le notifica que esa actividad puede ser constitutiva de la infracción penal menor de negligencia grave y, por último, la denuncia al Ministerio Fiscal para que se incoen diligencias penales por dicha infracción penal menor o por la infracción penal de vulneración del derecho de propiedad intelectual.

101 Se requiere asimismo que dicha normativa nacional establezca normas claras y precisas que garanticen que las direcciones IP conservadas de conformidad con la Directiva 2002/58 solo puedan utilizarse para identificar a la persona a la que se ha atribuido una determinada dirección IP, excluyendo una utilización que permita supervisar, mediante una o varias de esas direcciones, la actividad en línea de esa persona. Cuando una dirección IP se utiliza así con el solo propósito de identificar a su titular en el marco de un procedimiento administrativo específico que puede conducir a que se incoen contra él diligencias penales, y no con la finalidad, por ejemplo, de revelar los contactos o la localización de dicho titular, el acceso a esa dirección con ese solo propósito concierne a dicha dirección como dato de identidad civil en vez de como dato de tráfico.

102 Por añadidura, del principio consagrado en la jurisprudencia reiterada que se ha recordado en el apartado 97 de la presente sentencia se desprende que un acceso como aquel del que goza la Hadopi en virtud de la normativa nacional controvertida en el litigio principal, en tanto en cuanto persigue el objetivo de luchar contra las infracciones penales en general, solo puede justificarse si atañe a direcciones IP que los proveedores de servicios de comunicaciones electrónicas deban conservar en aras de ese mismo objetivo, y no en aras de un objetivo de mayor importancia como el de la lucha contra la delincuencia grave, sin perjuicio, no obstante, de un acceso justificado por tal objetivo de lucha contra las infracciones penales en general cuando atañe a direcciones IP almacenadas y por ende conservadas en las condiciones que se establecen en el artículo 6 de la Directiva 2002/58.

103 Asimismo, como se desprende de los apartados 85 a 92 de la presente sentencia, la conservación de direcciones IP, basada en una medida legislativa en virtud del artículo 15, apartado 1, de la Directiva 2002/58, en aras del objetivo de luchar contra las infracciones penales en general,

puede justificarse cuando las condiciones de dicha conservación fijadas por el régimen legal de que se trate observen un conjunto de exigencias destinadas a garantizar, en esencia, que las distintas categorías de datos conservados estén separadas en compartimentos estancos, de modo que se excluya efectivamente la asociación de datos pertenecientes a distintas categorías. En efecto, de imponerse tales condiciones de conservación a los proveedores de servicios de comunicaciones electrónicas, la conservación generalizada e indiferenciada de las direcciones IP no constituye injerencia grave en la vida privada de sus titulares por cuanto esos datos no permiten extraer conclusiones precisas sobre la vida privada de estos.

104 Por lo tanto, habida cuenta de la jurisprudencia recordada en los apartados 95 a 97 de la presente sentencia, en caso de que se establezca un régimen legal de estas características, el acceso a las direcciones IP conservadas en aras del objetivo de luchar contra las infracciones penales en general puede justificarse sobre la base del artículo 15, apartado 1, de la Directiva 2002/58 cuando ese acceso se autorice con el solo propósito de identificar a la persona sospechosa de estar implicada en tales infracciones.

105 Por lo demás, permitir que una autoridad pública como la Hadopi tenga acceso a datos de identidad civil correspondientes a una dirección IP pública que le ha sido transmitida por organizaciones de titulares de derechos con el solo propósito de identificar al titular de esa dirección utilizada para actividades que se hayan cometido en línea y que pudieran vulnerar los derechos de autor o los derechos afines a los derechos de autor, a fin de imponerle alguna de las medidas previstas en el marco del procedimiento de respuesta gradual, es conforme con la jurisprudencia del Tribunal de Justicia relativa al «derecho de información» en el contexto de los procedimientos relativos a una infracción del derecho de propiedad intelectual que se prevén en el artículo 8 de la Directiva 2004/48 (véase, en este sentido, la sentencia de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartados 47 y siguientes).

106 En efecto, en el marco de esta jurisprudencia, el Tribunal de Justicia, al tiempo que ha subrayado que la aplicación de las medidas previstas en la Directiva 2004/48 no puede afectar al RGPD ni a la Directiva 2002/58, ha declarado que el artículo 8, apartado 3, de la Directiva 2004/48, en relación con el artículo 15, apartado 1, de la Directiva 2002/58 y el artículo 7, letra f), de la Directiva 95/46, no se opone a que los Estados miembros impongan a los proveedores de servicios de comunicaciones electrónicas la obligación de transmisión a particulares de datos personales para permitir que se ejerzan acciones ante la jurisdicción civil contra las vulneraciones de los derechos de autor, aunque tampoco impone a esos Estado que establezcan tal obligación (véase, en este sentido, la sentencia de 17 de junio de 2021, M.I.C.M., C-597/19, EU:C:2021:492, apartados 124 y 125 y jurisprudencia citada).

107 Dicho esto, en segundo lugar, a los efectos de la apreciación concreta del grado de injerencia en la vida privada que supone el acceso de una autoridad pública a datos personales, no pueden dejar de tenerse en cuenta las particularidades del contexto en el que tiene lugar dicho acceso y, en particular, el conjunto de los datos y de la información que se comunican a dicha autoridad en virtud de la normativa nacional aplicable, incluidos los datos y la información preexistentes que revelen el contenido (véase, por analogía, TEDH, sentencia de 24 de abril de 2018, Benedik c. Eslovenia, CE:ECHR:2018:0424JUD006235714, § 109).

108 Así, en el presente asunto, es preciso tener en cuenta, a los efectos de dicha apreciación, que, con anterioridad al acceso a los datos de identidad civil en cuestión de que goza la Hadopi, esta recibe de las organizaciones de titulares de derechos, en particular, «información sobre las obras u objetos protegidos afectados por los hechos» y, «si procede», el «nombre del archivo tal y como se encuentra en la estación del abonado», a tenor del punto 1.° del anexo del Decreto n.º 2010-236.

109 De los autos que obran en poder del Tribunal de Justicia se desprende, a reserva, no obstante, de que el órgano jurisdiccional remitente compruebe este extremo, que la información sobre la obra en cuestión, tal como esa información se consigna en un acta cuyo contenido se delimita por las deliberaciones de la CNIL de 10 de junio de 2010, se circunscribe, esencialmente, al título de la obra de que se trate y a un extracto denominado «chunk» que se presenta como secuencia alfanumérica y no como registro de sonido o de vídeo de la obra.

110 A este respecto, es cierto que no puede excluirse, de manera general, que el acceso de una autoridad pública a un número limitado de datos de identidad civil del titular de una dirección IP que le haya comunicado un proveedor de servicios de comunicaciones electrónicas con el solo propósito de identificar a ese titular en el caso de que tal dirección se haya utilizado para actividades que pudieran vulnerar los derechos de autor o los derechos afines a los derechos de autor, si se asocia al análisis de información, aun limitada, sobre el contenido de la obra puesta ilegalmente a disposición en Internet que las organizaciones de titulares de derechos le hayan transmitido previamente, pueda dar a dicha autoridad pública información sobre determinados aspectos de la vida privada de dicho titular, incluidos datos sensibles, como la orientación sexual, las opiniones políticas, las convicciones religiosas, filosóficas, sociales o de otra índole, así como el estado de salud, datos estos que gozan además de especial protección en el Derecho de la Unión.

111 No obstante, en el presente asunto, habida cuenta de la naturaleza de los datos y de la información limitada de que dispone la Hadopi, solo en situaciones atípicas podrían esos datos e información revelar información, en su caso sensible, sobre aspectos de la vida privada de la persona de que se trate que, conjuntamente considerados, pudieran hacer posible que esa autoridad pública extrajera conclusiones precisas sobre su vida privada, por ejemplo estableciendo su perfil detallado.

112 Así podría suceder, en concreto, con una persona cuya dirección IP se haya utilizado para actividades que vulneran los derechos de autor o los derechos afines a los derechos de autor en redes entre pares repetidamente, o incluso a gran escala, en relación con obras protegidas de tipos particulares que puedan agruparse a partir de los términos de su título con potencial para revelar información, en su caso sensible, sobre aspectos de su vida privada.

113 Dicho esto, diversos elementos permiten considerar que, en el presente asunto, la injerencia en la vida privada de una persona sospechosa de haber realizado una actividad que vulnere los derechos de autor o los derechos afines a los derechos de autor que una normativa como la controvertida en el litigio principal autoriza no reviste necesariamente un nivel de gravedad elevado. Para empezar, conforme a tal normativa, el acceso de la Hadopi a los datos personales de que se trata se reserva a un número limitado de agentes jurados autorizados de dicha autoridad pública, órgano que goza además de un estatuto de independencia, conforme al artículo L. 331-12 del CPI. A continuación, ese acceso tiene como solo propósito identificar a una persona sospechosa de haber realizado una actividad que vulnere los derechos de autor o los derechos afines a los derechos de autor cuando se constata que se ha puesto ilegalmente a disposición desde su acceso a Internet una obra protegida.

Por último, el acceso de la Hadopi a los datos personales de que se trata se limita estrictamente a los datos necesarios a tal fin (véase, por analogía, TEDH, sentencia de 17 de octubre de 2019, López Ribalda y otros c. España, CE:ECHR:2019:1017JUD000187413, §§ 126 y 127).

114 Otro elemento que puede aminorar aún más el grado de injerencia en los derechos fundamentales a la protección de la vida privada y de los datos personales resultante de dicho acceso de la Hadopi, elemento que parece deducirse de los autos que obran en poder del Tribunal de Justicia, pero que corresponde comprobar al órgano jurisdiccional remitente, atañe a que, en virtud de la normativa nacional aplicable, los agentes de la Hadopi que disponen de acceso a los datos y a la información de que se trata tienen un deber de confidencialidad que les prohíbe divulgarlos de cualquier forma (salvo para denunciar los hechos al Ministerio Fiscal) y utilizarlos para fines distintos de la identificación del titular de una dirección IP sospechoso de haber realizado una actividad que vulnere los derechos de autor o los derechos afines a los derechos de autor en orden a imponerle alguna de las medidas contempladas en el marco del procedimiento de respuesta gradual (véase, por analogía, TEDH, sentencia de 17 de diciembre de 2009, Gardel c. Francia, CE:ECHR:2009:1217JUD001642805, § 70).

115 Así pues, siempre que una normativa nacional cumpla los requisitos recordados en el apartado 101 de la presente sentencia, las direcciones IP comunicadas a una autoridad pública como la Hadopi no permiten que se lleve a cabo un rastreo de la secuencia de navegación de su titular, lo que lleva a confirmar la apreciación de que no cabe calificar de grave la injerencia que supone el acceso de dicha autoridad a los datos de identificación en cuestión en el litigio principal.

116 En tercer lugar, ha de recordarse que, a los efectos de la necesaria conciliación entre los derechos e intereses en juego que impone la exigencia de proporcionalidad establecida en el artículo 15, apartado 1, primera frase, de la Directiva 2002/58, aun cuando la libertad de expresión y la confidencialidad de los datos personales son preocupaciones primordiales y los usuarios de las telecomunicaciones y de los servicios de Internet deben tener la garantía de que se respetarán su intimidad y su libertad de expresión, estos derechos fundamentales no son absolutos. En efecto, en el marco de la ponderación de los derechos e intereses en juego, estos deben en ocasiones ceder ante otros derechos fundamentales e imperativos de interés general, como la defensa del orden público y la prevención de las infracciones penales o la protección de los derechos y libertades de terceros. Así sucede, en particular, cuando la preponderancia que se reconoce a las referidas preocupaciones primordiales puede mermar la eficacia de una investigación penal, en particular haciendo imposible o excesivamente difícil que se identifique al autor de una infracción penal y se le imponga una sanción (véase, por analogía, TEDH, sentencia de 2 de marzo de 2009, K.U. c. Finlandia, CE:ECHR:2008:1202JUD000287202, § 49).

117 En este contexto, ha de tenerse debidamente en cuenta que, como ya ha declarado el Tribunal de Justicia, cuando se trata de infracciones cometidas en línea, el acceso a las direcciones IP puede constituir el único método de investigación para identificar a la persona que tenía atribuida esa dirección en el momento de la comisión de la infracción (véase, en este sentido, la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 154).

118 Esta circunstancia lleva a demostrar, como también señaló esencialmente el Abogado General en el punto 59 de sus conclusiones de 28 de septiembre de 2023, que la conservación de esas direcciones y el acceso a ellas son, cuando se trata de luchar contra infracciones penales como las que vulneran los derechos de autor o los derechos afines a los derechos de autor cometidas en

línea, estrictamente necesarios para la consecución del objetivo perseguido y, por tanto, cumplen la exigencia de proporcionalidad que impone el artículo 15, apartado 1, de la Directiva 2002/58, a la luz del considerando 11 de esta Directiva y del artículo 52, apartado 2, de la Carta.

119 No permitir tal acceso implicaría además, como esencialmente subrayó el Abogado General en los puntos 78 a 80 de sus conclusiones de 27 de octubre de 2022 y en los puntos 80 y 81 de sus conclusiones de 28 de septiembre de 2023, un riesgo real de impunidad sistémica no solo de infracciones penales que vulneran los derechos de autor o los derechos afines a los derechos de autor, sino también de otros tipos de infracciones penales cometidas en línea o cuya comisión o preparación se ve facilitada por las características propias de Internet. Pues bien, la existencia de tal riesgo constituye una circunstancia pertinente para apreciar, en el marco de la ponderación de los diferentes derechos e intereses en juego, si una injerencia en los derechos garantizados en los artículos 7, 8 y 11 de la Carta es una medida proporcionada respecto al objetivo de luchar contra las infracciones penales.

120 Es cierto que el acceso de una autoridad pública como la Hadopi a datos de identidad civil correspondientes a la dirección IP desde la que se cometió la infracción en línea no constituye necesariamente el único método de investigación posible para identificar a la persona que era titular de esa dirección en el momento de su comisión. En efecto, también cabría, *a priori*, realizar tal identificación examinando todas las actividades en línea de la persona de que se tratara, en particular analizando los «rastros» que hubiera podido dejar en las redes sociales, como el identificador utilizado en ellas o sus datos de contacto.

121 Sin embargo, como señaló el Abogado General en el punto 83 de sus conclusiones de 28 de septiembre de 2023, tal método de investigación sería especialmente invasivo, pues podría revelar información precisa sobre la vida privada de las personas de que se tratara. Así, supondría para ellas una injerencia en los derechos garantizados en los artículos 7, 8 y 11 de la Carta más grave que la que se deriva de una normativa como la controvertida en el litigio principal.

122 De las anteriores consideraciones se desprende que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que no se opone, en principio, a una normativa nacional que permite el acceso, por parte de una autoridad pública encargada de proteger los derechos de autor y los derechos afines a los derechos de autor contra las vulneraciones de esos derechos cometidas en Internet, a datos de identidad civil correspondientes a direcciones IP recabadas previamente por organizaciones de titulares de derechos y conservadas por los proveedores de servicios de comunicaciones electrónicas conforme a una separación en compartimentos estancos, con el solo propósito de que dicha autoridad pueda identificar a los titulares de esas direcciones sospechosos de ser responsables de tales vulneraciones y, en su caso, pueda adoptar medidas contra ellos. En tal caso, la normativa nacional aplicable debe prohibir a los agentes que dispongan de tal acceso, primero, divulgar de cualquier forma información sobre el contenido de los archivos consultados por esos titulares, salvo a los solos efectos de presentar denuncia ante el Ministerio Fiscal, segundo, realizar cualquier rastreo de la secuencia de navegación de esos titulares y, tercero, utilizar esas direcciones IP con fines distintos de la adopción de esas medidas.

Sobre la exigencia de control previo de un órgano jurisdiccional o una entidad administrativa independiente antes de que una autoridad pública acceda a datos de identidad civil correspondientes a una dirección IP

123 Con todo, se plantea la cuestión de si el acceso de la autoridad pública a datos de identidad civil correspondientes a una dirección IP debe condicionarse, además, al control previo de un órgano jurisdiccional o de una entidad administrativa independiente.

124 A este respecto, para garantizar en la práctica el íntegro cumplimiento de los requisitos que los Estados miembros están obligados a establecer para garantizar que el acceso se limite a lo estrictamente necesario, el Tribunal de Justicia ha declarado que es «esencial» que el acceso de las autoridades nacionales competentes a los datos de tráfico y a los datos de localización se supedite a un control previo efectuado por un órgano jurisdiccional o por una entidad administrativa independiente [véanse, en este sentido, las sentencias de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartado 120; de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 189; de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 51, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 106].

125 Este control previo requiere, en primer término, que el órgano jurisdiccional o la entidad administrativa independiente encargada de efectuarlo disponga de todas las atribuciones y presente todas las garantías necesarias para conciliar los diferentes intereses legítimos y derechos de que se trate. En el caso concreto de una investigación penal, tal control exige que ese órgano jurisdiccional o esa entidad esté en condiciones de ponderar adecuadamente, por una parte, los intereses legítimos relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales que asisten a las personas a cuyos datos se pretende acceder (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 107 y jurisprudencia citada).

126 En segundo término, cuando dicho control no lo lleve a cabo un órgano jurisdiccional, sino una entidad administrativa independiente, esta última debe gozar de un estatuto que le permita actuar en el ejercicio de sus funciones con objetividad e imparcialidad y, para ello, ha de estar a resguardo de toda influencia externa. De esta manera, el requisito de independencia que debe cumplir la entidad que ejerce el control previo obliga a que tenga la condición de tercero respecto del órgano que solicita el acceso a los datos, de modo que la primera pueda ejercer ese control con objetividad e imparcialidad, y a resguardo de toda influencia externa. En particular, en el ámbito penal, el requisito de independencia implica que la autoridad que ejerce ese control previo, por una parte, no esté implicada en la realización de la investigación penal de que se trate y, por otra parte, que tenga una posición neutral frente a las partes del procedimiento penal (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 108 y jurisprudencia citada).

127 En tercer término, el control independiente exigido con arreglo al artículo 15, apartado 1, de la Directiva 2002/58 debe realizarse antes de cualquier acceso a los datos en cuestión, salvo en caso de urgencia debidamente justificada, supuesto en el cual el control debe efectuarse en breve plazo. En efecto, un control ulterior no permitiría cumplir el objetivo del control previo, que consiste en

impedir que se autorice un acceso a los datos en cuestión que exceda de los límites de lo estrictamente necesario [sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 110].

128 Sentado lo anterior, si bien, como se desprende de la jurisprudencia recordada en el apartado 124 de la presente sentencia, el Tribunal de Justicia ha considerado «esencial» que el acceso de las autoridades nacionales competentes a los datos de tráfico y a los datos de localización se someta al control previo de un órgano jurisdiccional o de una entidad administrativa independiente, esa jurisprudencia se ha desarrollado en el contexto de ciertas medidas nacionales que permitían, en aras de un objetivo ligado a la lucha contra la delincuencia grave, el acceso general a todos los datos de tráfico y de localización conservados, con independencia de cualquier vínculo, aunque solo fuera indirecto, con la finalidad perseguida, y que de esta manera implicaban injerencias graves e incluso «especialmente graves» en los derechos fundamentales afectados.

129 En cambio, cuando han sido materia de controversia las condiciones en las que el acceso a los datos de identidad civil podía justificarse en virtud del artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7, 8 y 11 de la Carta, el Tribunal de Justicia no ha hecho mención expresa alguna a tal control previo [véanse, en este sentido, las sentencias de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartados 59, 60 y 62; de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 157 y 158, y de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 34].

130 Pues bien, de la jurisprudencia del Tribunal de Justicia relativa al principio de proporcionalidad, cuya observancia exige el artículo 15, apartado 1, primera frase, de la Directiva 2002/58, en particular de aquella según la cual la posibilidad de que los Estados miembros justifiquen una limitación de los derechos y obligaciones que se recogen, en particular, en los artículos 5, 6 y 9 de dicha Directiva, debe apreciarse determinando la gravedad de la injerencia en los artículos 7, 8 y 11 de la Carta que supone esa limitación y comprobando que la importancia del objetivo de interés general perseguido por dicha limitación guarde relación con tal gravedad (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 131), se desprende que el grado de injerencia en los derechos fundamentales en cuestión que supone el acceso a los datos personales de que se trate y el nivel de sensibilidad de los mismos también deben influir en las garantías materiales y procedimentales que han de imponerse a dicho acceso, entre las que figura la exigencia del control previo de un órgano jurisdiccional o de una entidad administrativa independiente.

131 Consiguientemente, habida cuenta de este principio de proporcionalidad, se ha de considerar que la exigencia del control previo de un órgano jurisdiccional o de una entidad administrativa independiente se impone cuando, en el contexto de una normativa nacional que contempla el acceso de una autoridad pública a datos personales, ese acceso entrañe el riesgo de que se produzca una injerencia grave en los derechos fundamentales de la persona afectada, en el sentido de que podría posibilitar que dicha autoridad pública extraiga conclusiones precisas sobre su vida privada y, en su caso, establezca un perfil detallado de ella.

132 A la inversa, esa exigencia de control previo no resulta de aplicación cuando la injerencia en los derechos fundamentales en cuestión que supone el acceso de una autoridad pública a datos personales no pueda calificarse de grave.

133 Así sucede con el acceso a datos de identidad civil de los usuarios de los medios de comunicaciones electrónicas con el solo propósito de identificar al usuario en cuestión y sin que esos datos puedan asociarse a información sobre las comunicaciones realizadas, puesto que, según el Tribunal de Justicia, la injerencia que supone tal tratamiento de dichos datos no puede, en principio, calificarse de grave (véase, en este sentido, la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 157 y 158).

134 De lo anterior se sigue que, en caso de que se establezca un sistema de conservación como el descrito en los apartados 86 a 89 de la presente sentencia, el acceso de la autoridad pública a los datos de identidad civil correspondientes a las direcciones IP conservadas de esta manera no se condiciona, en principio, a la exigencia de control previo de un órgano jurisdiccional o de una entidad administrativa independiente.

135 Dicho esto, como ya se ha señalado en los apartados 110 y 111 de la presente sentencia, no puede excluirse que, en situaciones atípicas, la información y datos limitados que se pongan a disposición de una autoridad pública en el marco de un procedimiento como el de respuesta gradual controvertido en el litigio principal puedan revelar informaciones, en su caso sensibles, sobre aspectos de la vida privada de la persona afectada, informaciones que, conjuntamente consideradas, podrían permitir a esa autoridad pública extraer conclusiones precisas sobre su vida privada y, en su caso, establecer su perfil detallado.

136 Como se desprende del apartado 112 de la presente sentencia, tal riesgo para la vida privada puede presentarse, en particular, cuando una persona realiza actividades que vulneran los derechos de autor o los derechos afines a los derechos de autor en redes entre pares repetidamente, o incluso a gran escala, en relación con obras protegidas de clases particulares susceptibles de agruparse a partir de los términos de su título que revelen información, en su caso sensible, sobre su vida privada.

137 Así, en el presente asunto, en el procedimiento administrativo de respuesta gradual, un titular de una dirección IP puede estar particularmente expuesto a tal riesgo para su vida privada cuando se alcanza la fase en que la Hadopi tiene que decidir si denuncia o no los hechos al Ministerio Fiscal para que se incoen contra él diligencias por hechos que pudieran ser constitutivos de la infracción penal menor de negligencia grave o de la infracción penal de vulneración del derecho de propiedad intelectual.

138 En efecto, esa denuncia al Ministerio Fiscal presupone que ya se hayan remitido a dicho titular dos recomendaciones y una notificación en que se lo informa de que sus actividades pueden dar lugar a acciones penales, medidas que implican que, en cada ocasión, la Hadopi haya tenido acceso a datos de identidad civil de dicho titular cuya dirección IP se haya utilizado para actividades que vulneren los derechos de autor o los derechos afines a los derechos de autor, así como a un archivo referente a dicha obra que contiene, esencialmente, el título de esta.

139 Pues bien, no cabe excluir que, considerados conjuntamente y a medida que va avanzando el procedimiento administrativo de respuesta gradual, los datos que de tal manera se facilitan en las diferentes fases de este procedimiento puedan revelar información concordante y, en su caso, sensible sobre aspectos de la vida privada de la persona de que se trate que, en su caso, permita establecer su perfil.

140 Así pues, la intensidad del menoscabo del derecho al respeto de la vida privada puede incrementarse a medida que el procedimiento de respuesta gradual, que se desarrolla secuencialmente, vaya avanzando por sus distintas fases.

141 En el presente asunto, el acceso de la Hadopi al conjunto de los datos de la persona de que se trate acumulados a lo largo de las distintas fases de que consta ese procedimiento puede posibilitar, si se los asocia, que se extraigan conclusiones precisas sobre su vida privada. Por tanto, en un procedimiento como el de respuesta gradual objeto del litigio principal, la normativa nacional debe contemplar asimismo, en alguna fase determinada de dicho procedimiento, un control previo de un órgano jurisdiccional o de una entidad administrativa independiente que se adecúe a los requisitos recordados en los apartados 125 a 127 de la presente sentencia, en orden a descartar riesgos de injerencias desproporcionadas en los derechos fundamentales a la protección de la vida privada y de los datos personales de la persona afectada. Lo anterior significa que, en la práctica, tal control debe realizarse antes de que la Hadopi pueda asociar datos de identidad civil de una persona que correspondan a una dirección IP y que se hayan obtenido de un proveedor de servicios de comunicaciones electrónicas —persona que ya haya recibido dos recomendaciones— al archivo referente a la obra que se haya puesto a disposición en Internet con la finalidad de que otras personas la descarguen. Consiguientemente, dicho control debe realizarse antes de la notificación, a que se refiere el artículo R. 331-40 del CPI, en que se indica que esa persona ha cometido hechos que pudieran ser constitutivos de la infracción penal menor de negligencia grave. Solo una vez que se haya realizado el control previo de un órgano jurisdiccional o de una autoridad administrativa independiente y se haya obtenido autorización de ese órgano o entidad podrá remitir la Hadopi esa notificación y, posteriormente, si procede, denunciar los hechos al Ministerio Fiscal para que se incoen diligencias penales por esa infracción.

142 Ha de permitirse a la Hadopi identificar los casos en que el titular de la dirección IP de que se trate alcanza esa tercera fase de tal procedimiento de respuesta gradual. Por tanto, ese procedimiento debe organizarse y estructurarse de manera que los datos de identidad civil de una persona correspondientes a direcciones IP que se hayan recogido previamente en Internet y que los proveedores de servicios de comunicaciones electrónicas hayan facilitado no puedan automáticamente ser asociados, por las personas encargadas del examen de los hechos en la Hadopi, a los archivos en que figuran los elementos que permiten conocer los títulos de las obras protegidas cuya puesta a disposición en Internet haya justificado esa recogida.

143 Así pues, la referida asociación a los efectos de la tercera fase de la respuesta gradual debe suspenderse cuando la recogida de dichos datos de identidad civil, respecto de un caso de posible segunda repetición de una actividad que vulnere los derechos de autor o los derechos afines a los derechos de autor, active la exigencia del control previo de un órgano jurisdiccional o de una entidad administrativa independiente que se ha descrito en el apartado 141 de la presente sentencia.

144 Por otra parte, la modulación de la exigencia de control previo que se ha expuesto en los apartados 141 a 143 de la presente sentencia, en el sentido de que se circunscribe a la tercera fase de dicho procedimiento de respuesta gradual y no se aplica a las fases anteriores del mismo, también posibilita que se tome en consideración el argumento que propugna que ha de salvaguardarse la practicabilidad del referido procedimiento, que se caracteriza —especialmente en las fases anteriores a la remisión de la notificación y, en su caso, a la denuncia al Ministerio Fiscal— por el carácter masivo de las solicitudes de acceso de la autoridad pública como resultado del número igualmente elevado de actas que las organizaciones de titulares de derechos transmiten a esta autoridad.

145 Por lo que respecta al objeto del control previo a que se ha hecho referencia en los apartados 141 a 143 de la presente sentencia, de la jurisprudencia recordada en los apartados 95 y 96 de dicha sentencia se desprende que, en los casos en que existen sospechas de que la persona en cuestión ha cometido la infracción penal menor de «negligencia grave» del artículo R. 335-5 del CPI, comprendida en las infracciones penales en general, el órgano jurisdiccional o la entidad administrativa independiente a cargo de dicho control debe denegar el acceso cuando este permita que la autoridad pública que lo haya solicitado extraiga conclusiones precisas sobre la vida privada de esa persona.

146 En cambio, incluso un acceso que haga posible extraer semejantes conclusiones precisas debería autorizarse en los casos en los que los elementos que se pongan en conocimiento de dicho órgano jurisdiccional o entidad administrativa independiente permitan sospechar que la persona en cuestión ha cometido la infracción penal de vulneración del derecho de propiedad intelectual tipificada en el artículo L. 335-2 del CPI o en el artículo L. 335-4 del mismo, habida cuenta de que un Estado miembro puede considerar que la referida infracción penal, en tanto en cuanto afecta a un interés fundamental de la sociedad, se encuadra en las formas graves de delincuencia.

147 Por último, por lo que atañe a la forma de realización de tal control previo, el Gobierno francés estima que, en vista de las características particulares del acceso de la Hadopi a los datos en cuestión, en concreto de su carácter masivo, procedería, de ser indispensable ese control previo, que fuera totalmente automatizado. Según dicho Gobierno, tal control, de carácter puramente objetivo, tendría esencialmente por objeto comprobar que el acta remitida a la Hadopi contuviese toda la información y los datos requeridos sin que esta autoridad hubiera de valorar esa información y esos datos.

148 Sin embargo, el control previo no puede en ningún caso automatizarse totalmente, ya que, como se desprende de la jurisprudencia recordada en el apartado 125 de la presente sentencia, cuando se trata de una investigación penal, tal control exige, en cualquier caso, que el órgano jurisdiccional o la entidad administrativa independiente de que se trate esté en condiciones de ponderar adecuadamente, por una parte, los intereses legítimos relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales que asisten a las personas a cuyos datos se pretende acceder.

149 En efecto, tal ponderación de los diferentes intereses legítimos y de los derechos afectados requiere la intervención de una persona física, que es tanto más necesaria cuanto que la automaticidad y el carácter masivo del tratamiento de datos de que se trata comportan riesgos para la vida privada.

150 Además, un control totalmente automatizado no permite, en principio, garantizar que el acceso no exceda los límites de lo estrictamente necesario y que las personas cuyos datos personales se vean afectados dispongan de garantías efectivas contra los riesgos de abuso y contra cualquier acceso y uso ilícitos de esos datos.

151 De este modo, si bien determinados controles automatizados pueden permitir comprobar algunos de los datos incluidos en las actas de las organizaciones de titulares de derechos, tales controles deben, en cualquier caso, acompañarse de controles realizados por personas físicas que cumplan plenamente las exigencias recordadas en los apartados 125 a 127 de la presente sentencia.

Sobre las exigencias relativas a los requisitos materiales y procedimentales y a las garantías contra los riesgos de abuso y contra cualquier acceso o uso ilícitos de esos datos que se imponen al acceso de una autoridad pública a datos de identidad civil correspondientes a una dirección IP

152 De la jurisprudencia del Tribunal de Justicia se desprende que el acceso a datos personales solamente se ajusta a la exigencia de proporcionalidad que impone el artículo 15, apartado 1, de la Directiva 2002/58 si la medida legislativa que lo autoriza contempla, con reglas claras y precisas, que dicho acceso se supedite al cumplimiento de los correspondientes requisitos materiales y procedimentales y que las personas afectadas dispongan de garantías efectivas contra los riesgos de acceso y de uso abusivos o ilícitos de esos datos [véanse, en este sentido, las sentencias de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartados 132 y 173, y de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 49 y jurisprudencia citada].

153 Como ha subrayado el Tribunal de Justicia, la necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 176 y jurisprudencia citada).

154 A este respecto, en respuesta a una pregunta que el Tribunal de Justicia formuló para que se respondiera en la vista de 5 de julio de 2022, el Gobierno francés confirmó que, como por lo demás se indica en el artículo L. 331-29 del CPI, el acceso de la Hadopi a los datos de identidad civil en el marco del procedimiento de respuesta gradual procede de un tratamiento de datos esencialmente automatizado que se explica porque son masivas las vulneraciones del derecho de propiedad intelectual que las entidades de titulares de derechos constatan en las redes entre pares, constataciones que se transmiten a la Hadopi mediante actas.

155 Se desprende concretamente de los autos que obran en poder del Tribunal de Justicia que, con ocasión de ese tratamiento de datos, los agentes de la Hadopi comprueban, de manera esencialmente automatizada y sin valorar los hechos de que se trata en sí, si las actas que se le transmiten contienen toda la información y todos los datos relacionados en el punto 1.° del anexo del Decreto n.º 2010-236, en particular los hechos consistentes en poner ilegalmente a disposición obras y otros objetos en Internet y las direcciones IP utilizadas a tal fin. Pues bien, tales tratamientos deben acompañarse de controles realizados por personas físicas.

156 Habida cuenta de que tal tratamiento automatizado puede comportar un determinado número de falsos positivos y, sobre todo, el riesgo de que un número de datos personales que puede llegar a ser muy elevado sean desviados por terceros para finalidades abusivas o ilícitas, es preciso que, en virtud de una medida legislativa, el sistema de tratamiento de datos utilizado por una autoridad pública se someta, periódicamente, al control de un organismo que sea independiente y tenga la condición de tercero respecto de dicha autoridad, en orden a comprobar la integridad del sistema, incluidas las garantías efectivas contra los riesgos de abuso y contra cualquier acceso y uso ilícitos de esos datos que dicho sistema debe asegurar, así como su eficacia y fiabilidad para detectar los ilícitos que, en caso de reiteración, pueden calificarse de negligencia grave o de vulneración del derecho de propiedad intelectual.

157 Por último, es preciso añadir que un tratamiento de datos personales efectuado por una autoridad pública, como el que realiza la Hadopi en el procedimiento de respuesta gradual, debe atenerse a las normas específicas de protección de esos datos que se contemplan en la Directiva 2016/680,

que, según su artículo 1, tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

158 En efecto, en el presente asunto, aun cuando, en virtud del Derecho nacional aplicable, no dispone de potestades de decisión propias, la Hadopi, cuando trata, en el procedimiento de respuesta gradual, datos personales y adopta medidas como la recomendación o la información a la persona afectada de que los hechos de que se trata pueden dar lugar a acciones penales, debe calificarse de «autoridad pública», en el sentido del artículo 3 de la Directiva 2016/680, que participa en la prevención y la detección de infracciones penales, a saber, la infracción penal menor de negligencia grave o la infracción penal de vulneración del derecho de propiedad intelectual, y, por tanto, entra en el ámbito de aplicación de esta Directiva de conformidad con su artículo 1.

159 A este respecto, en respuesta a una pregunta que formuló el Tribunal de Justicia para que se respondiera en la vista de 5 de julio de 2022, el Gobierno francés indicó que, como las medidas adoptadas por la Hadopi en el marco de la aplicación del procedimiento de respuesta gradual «tienen un carácter previo a la vía penal y directamente relacionado con el proceso judicial», el sistema de gestión de las medidas para la protección de las obras en Internet que aplica la Hadopi está sujeto, como se desprende de la jurisprudencia del órgano jurisdiccional remitente, a las disposiciones de Derecho nacional de transposición de la Directiva 2016/680.

160 En cambio, tal tratamiento de datos por parte de la Hadopi no está comprendido en el ámbito de aplicación del RGPD. En efecto, el artículo 2, apartado 2, letra d), del RGPD establece que este último no se aplica al tratamiento de datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

161 Como señaló el Abogado General en el punto 104 de sus conclusiones de 27 de octubre de 2022, dado que la Hadopi viene obligada a respetar la Directiva 2016/680 en el marco del procedimiento de respuesta gradual, las personas implicadas en tal procedimiento deben disfrutar de un conjunto de garantías materiales y procedimentales que engloban el derecho de acceso, de rectificación y de supresión de los datos personales tratados por la Hadopi, así como la posibilidad de presentar una reclamación ante una autoridad de control independiente, seguida, en su caso, de un recurso judicial interpuesto con arreglo a las condiciones de Derecho común.

162 En este contexto, de la legislación nacional controvertida en el litigio principal se desprende que, en el marco del procedimiento de respuesta gradual, más concretamente cuando se envía la segunda recomendación y cuando se remite la posterior notificación en que se indica que los hechos constatados pueden ser calificados de infracción penal, el destinatario de esas comunicaciones goza de determinadas garantías procedimentales, como el derecho a presentar alegaciones, el derecho a que se le faciliten detalles sobre el ilícito que se le imputa y, en el caso de que se le remita dicha notificación, el derecho a solicitar una audiencia y a estar asistido por un abogado.

163 En cualquier caso, corresponde al órgano jurisdiccional remitente comprobar si esta normativa nacional comprende el conjunto de garantías materiales y procedimentales que la Directiva 2016/680 prescribe.

164 Habida cuenta de todas las consideraciones que anteceden, ha de responderse a las tres cuestiones prejudiciales que el artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que no se opone a una normativa nacional que autoriza a la autoridad pública encargada de proteger los derechos de autor y los derechos afines a los derechos de autor contra las vulneraciones de esos derechos cometidas en Internet a acceder a los datos, conservados por los proveedores de servicios de comunicaciones electrónicas accesibles para el público, de identidad civil correspondientes a direcciones IP recabadas previamente por organizaciones de titulares de derechos, con el propósito de que dicha autoridad pública pueda identificar a los titulares de esas direcciones, utilizadas para actividades que pudieran ser constitutivas de tales vulneraciones, y, en su caso, pueda adoptar medidas contra ellos, siempre que, en virtud de esa normativa,

– esos datos se conserven en unas condiciones y conforme a un sistema técnico que garanticen que se excluya que dicha conservación posibilite extraer conclusiones precisas sobre la vida privada de esos titulares, por ejemplo estableciendo su perfil detallado, lo que puede conseguirse, en particular, imponiendo a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar las diferentes categorías de datos personales, como los datos de identidad civil, las direcciones IP y los datos de tráfico y los datos de localización, de una manera que asegure una separación en compartimentos estancos de esas diferentes categorías de datos que impida, en la fase de la conservación, cualquier explotación conjunta de esas diferentes categorías de datos, y por un período que no exceda de lo estrictamente necesario;

– el acceso de esta autoridad pública a tales datos conservados conforme a una separación en compartimentos estancos sirva exclusivamente para identificar a la persona sospechosa de haber cometido una infracción penal y cuente con las garantías necesarias para excluir que, fuera de las situaciones atípicas, ese acceso pueda permitir que se extraigan conclusiones precisas sobre la vida privada de los titulares de las direcciones IP, por ejemplo estableciendo su perfil detallado, lo que implica, en particular, que los agentes de dicha autoridad autorizados para ese acceso tengan prohibido divulgar de cualquier modo información sobre el contenido de los archivos consultados por esos titulares (salvo con el solo propósito de denunciar los hechos al Ministerio Fiscal), rastrear la secuencia de navegación de dichos titulares y, de manera más general, utilizar esas direcciones IP para fines distintos de la identificación de sus titulares en orden a la posible adopción de medidas contra ellos;

– la posibilidad de que las personas encargadas del examen de los hechos en dicha autoridad pública asocien tales datos a los archivos que contengan elementos que permitan conocer el título de obras protegidas cuya puesta a disposición en Internet haya justificado la recogida de las direcciones IP por parte de organizaciones de titulares de derechos se condicione, en los casos en que la misma persona vuelva a reiterar una actividad que vulnere los derechos de autor o los derechos afines a los derechos de autor, al control de un órgano jurisdiccional o una entidad administrativa independiente, que no puede automatizarse totalmente y que debe efectuarse antes de que se realice esa asociación, la cual, en tales casos, puede permitir que se extraigan conclusiones precisas sobre la vida privada de dicha persona cuya dirección IP se haya utilizado para actividades que pudieran ser constitutivas de vulneración de los derechos de autor o los derechos afines a los derechos de autor;

– el sistema de tratamiento de datos utilizado por la autoridad pública se someta periódicamente al control de un organismo que sea independiente y tenga la condición de tercero respecto de dicha autoridad pública, en orden a comprobar la integridad del sistema, incluidas las garantías efectivas contra los riesgos de acceso y uso abusivos o ilícitos de dichos datos, así como su eficacia y fiabilidad para detectar los posibles ilícitos.

Costas

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

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

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, a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea,

debe interpretarse en el sentido de que

no se opone a una normativa nacional que autoriza a la autoridad pública encargada de proteger los derechos de autor y los derechos afines a los derechos de autor contra las vulneraciones de esos derechos cometidas en Internet a acceder a los datos, conservados por los proveedores de servicios de comunicaciones electrónicas accesibles para el público, de identidad civil correspondientes a direcciones IP recabadas previamente por organizaciones de titulares de derechos, con el propósito de que dicha autoridad pública pueda identificar a los titulares de esas direcciones, utilizadas para actividades que pudieran ser constitutivas de tales vulneraciones, y, en su caso, pueda adoptar medidas contra ellos, siempre que, en virtud de esa normativa,

– **esos datos se conserven en unas condiciones y conforme a un sistema técnico que garanticen que se excluya que dicha conservación posibilite extraer conclusiones precisas sobre la vida privada de esos titulares, por ejemplo estableciendo su perfil detallado, lo que puede conseguirse, en particular, imponiendo a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar las diferentes categorías de datos personales, como los datos de identidad civil, las direcciones IP y los datos de tráfico y los datos de localización, de una manera que asegure una separación en compartimentos estancos de esas diferentes categorías de datos que impida, en la fase de la conservación, cualquier explotación conjunta de esas diferentes categorías de datos, y por un período que no exceda de lo estrictamente necesario;**

– **el acceso de esta autoridad pública a tales datos conservados conforme a una separación en compartimentos estancos sirva exclusivamente para identificar a la persona sospechosa de haber cometido una infracción penal y cuente con las garantías necesarias**

para excluir que, fuera de las situaciones atípicas, ese acceso pueda permitir que se extraigan conclusiones precisas sobre la vida privada de los titulares de las direcciones IP, por ejemplo estableciendo su perfil detallado, lo que implica, en particular, que los agentes de dicha autoridad autorizados para ese acceso tengan prohibido divulgar de cualquier modo información sobre el contenido de los archivos consultados por esos titulares (salvo con el solo propósito de denunciar los hechos al Ministerio Fiscal), rastrear la secuencia de navegación de dichos titulares y, de manera más general, utilizar esas direcciones IP para fines distintos de la identificación de sus titulares en orden a la posible adopción de medidas contra ellos;

– **la posibilidad de que las personas encargadas del examen de los hechos en dicha autoridad pública asocien tales datos a los archivos que contengan elementos que permitan conocer el título de obras protegidas cuya puesta a disposición en Internet haya justificado la recogida de las direcciones IP por parte de organizaciones de titulares de derechos se condicione, en los casos en que la misma persona vuelva a reiterar una actividad que vulnere los derechos de autor o los derechos afines a los derechos de autor, al control de un órgano jurisdiccional o una entidad administrativa independiente, que no puede automatizarse totalmente y que debe efectuarse antes de que se realice esa asociación, la cual, en tales casos, puede permitir que se extraigan conclusiones precisas sobre la vida privada de dicha persona cuya dirección IP se haya utilizado para actividades que pudieran ser constitutivas de vulneración de los derechos de autor o los derechos afines a los derechos de autor;**

– **el sistema de tratamiento de datos utilizado por la autoridad pública se someta periódicamente al control de un organismo que sea independiente y tenga la condición de tercero respecto de dicha autoridad pública, en orden a comprobar la integridad del sistema, incluidas las garantías efectivas contra los riesgos de acceso y uso abusivos o ilícitos de dichos datos, así como su eficacia y fiabilidad para detectar los posibles ilícitos.**

Firmas