SENTENCIA DEL TRIBUNAL (Pleno)

30 de abril de 2024 (*)

Tabla de contenido

Costos

(Petición de decisión prejudicial – Tratamiento de 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 Unión Europea – Artículos 7, 8 y 11 y artículo 52, apartado 1 – Legislación nacional destinada a combatir, mediante la intervención de una autoridad pública, los delitos de falsificación cometidos en Internet – Procedimiento de «respuesta gradual» – Recopilación inicial por parte de organizaciones de titulares de derechos de propiedad intelectual direcciones utilizadas para actividades que infringen los derechos de autor o derechos afines – Acceso posterior por parte de la autoridad pública responsable de la protección de los derechos de autor y derechos afines a los datos relacionados con la identidad civil asociados con esas direcciones IP conservadas por los proveedores de servicios de comunicaciones electrónicas – Procesamiento automatizado – Requisito de revisión previa por un tribunal o un organismo administrativo independiente – Condiciones sustantivas y procesales – Salvaguardias contra los riesgos de abuso y contra cualquier acceso o uso ilegal de esos datos)

En el asunto C-470/21,

SOLICITUD de decisión prejudicial presentada por el Conseil d'État (Consejo de Estado, Francia) con arreglo al artículo 267 TFUE mediante resolución de 5 de julio de 2021, recibida en el Tribunal de Justicia el 30 de julio de 2021, en el procedimiento

La cuadratura de la red,

Federación de facilitadores de acceso a asociados de Internet,

Franciliens.net,

Red de datos francesa

v

primer ministro,

Ministro de la Cultura,

EL TRIBUNAL (Pleno)

compuesto por K. Lenaerts, Presidente, L. Bay Larsen, Vicepresidente, A. Arabadjiev, A. Prechal (Ponente), K. Jürimäe, C. Lycourgos, E. Regan, T. von Danwitz, F. Biltgen, N Piçarra y Z. Csehi, Presidentes de Sala, M. Ilešič, J.-C. Bonichot, S. Rodin, PG Xuereb, LS Rossi, I. Jarukaitis, A. Kumin, N. Jääskinen, N. Wahl, I. Ziemele, J. Passer, D. Gratsias, ML Arastey Sahún y M. Gavalec, Jueces,

Abogado General: Sr. Szpunar,

Registradores: V. Giacobbo y M. Krausenböck, Administradores,

Visto el procedimiento escrito y celebrada la vista el 5 de julio de 2022,

después de considerar las observaciones presentadas en nombre de:

– La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net y French Data Network, por A. Fitzjean Ó Cobhthaigh, abogado,

– el Gobierno francés, en nombre de A. Daniel, A.-L. Desjonquères y J. Illouz, en calidad de agentes,

– el Gobierno danés, en nombre de JF Kronborg y V. Pasternak Jørgensen, en calidad de agentes,

– el Gobierno estonio, en nombre del Sr. Kriisa, en calidad de agente,

– el Gobierno finlandés, en nombre de H. Leppo, en calidad de agente,

– el Gobierno sueco, en nombre de H. Shev, en calidad de agente,

– el Gobierno noruego, en nombre de F. Bergsjø, S.-E. Dahl, JT Kaasin y P. Wennerås, en calidad de agentes,

– la Comisión Europea, en nombre de SL Kalėda, H. Kranenborg, P.-J. Loewenthal y F. Wilman, en calidad de agentes,

oídas las conclusiones del Abogado General en la sesión del 27 de octubre de 2022,

Visto el auto de 23 de marzo de 2023 de reapertura de la fase oral, y previa la audiencia de 15 de mayo de 2023,

después de considerar las observaciones presentadas en nombre de:

– La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net y French Data Network, por A. Fitzjean Ó Cobhthaigh, abogado,

– el Gobierno francés, en nombre de R. Bénard, J. Illouz y T. Stéhelin, en calidad de agentes,

– el Gobierno checo, en nombre de T. Suchá y J. Vláčil, en calidad de agentes,

– el Gobierno danés, por los representantes JF Kronborg y CA-S. Maertens, en calidad de Agentes,

– el Gobierno estonio, en nombre del Sr. Kriisa, en calidad de agente,

– Irlanda, por los Sres. M. Browne, Chief State Solicitor, A. Joyce y D. O'Reilly, en calidad de agentes, y por D. Fenelly, Barrister-at-Law,

– el Gobierno español, en nombre de A. Gavela Llopis, en calidad de Agente,

– el Gobierno chipriota, por el Sr. I. Neophytou, en calidad de Agente,

– el Gobierno letón, en nombre de J. Davidoviča y K. Pommere, en calidad de agentes,

– el Gobierno neerlandés, en nombre de EMM Besselink, MK Bultermann y A. Hanje, en calidad de agentes,

– el Gobierno finlandés, en nombre de A. Laine y H. Leppo, en calidad de agentes,

– el Gobierno sueco, en nombre de F.-D. Göransson y H. Shev, en calidad de agentes,

– el Gobierno noruego, en nombre de S.-E. Dahl y P. Wennerås, en calidad de agentes,

– la Comisión Europea, en nombre de SL Kalėda, H. Kranenborg, P.-J. Loewenthal y F. Wilman, en calidad de agentes,

– el Supervisor Europeo de Protección de Datos, en nombre de V. Bernardo, C.-A. Marnier, D. Nardi y M. Pollmann, en calidad de agentes,

– Agencia de Ciberseguridad de la Unión Europea (ENISA), en nombre de A. Bourka, en calidad de Agente,

oídas las conclusiones del Abogado General en la sesión del 28 de septiembre de 2023,

da lo siguiente

Juicio

1 La presente 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, sobre el tratamiento de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y comunicaciones electrónicas) (DO 2002, L 201, p. 37), 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) («Directiva 2002/ 58'), leído a la luz de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, "la Carta").

2 La solicitud se presentó en el marco de un litigio entre las asociaciones La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net y French Data Network, por una parte, y el Premier ministre (Primer Ministro, Francia) y el ministre de la Culture (Ministro de Cultura, Francia), por otra parte, en relación con la legalidad del decreto n º 2010-236, del 5 de marzo de 2010, relativo al trato automatizado de données à caractère personal autorizado por el artículo L. 331-29 del code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la Protection des œuvres sur internet » (Decreto nº 2010-236, de 5 de marzo de 2010, sobre el sistema automatizado de tratamiento de datos personales autorizado por el artículo L. 331-29 del el code de la propriété intellectuelle (Código de propiedad intelectual), denominado «Sistema de gestión de las medidas de protección de las obras en Internet» (JORF nº 56 de 7 de marzo de 2010, texto nº 19), modificado por el decreto n. de 2017-924, del 6 de mayo de 2017, relativo a la gestión de los derechos de autor y de los derechos de autor por un organismo de gestión de derechos y modificante del código de propiedad intelectual (Decreto n.º 2017-924, de 6 de mayo de 2017, sobre el gestión de los derechos de autor y derechos afines por una entidad de gestión de derechos y por la que se modifica el Código de Propiedad Intelectual) (JORF n.º 109, de 10 de mayo de 2017, texto n.º 176) (en lo sucesivo, «Decreto n.º 2010-236»).

Contexto legal

Derecho de la Unión Europea

Normas generales relativas a la protección de datos personales

– *Directiva 95/46/CE*

3 Artículo 7 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), contenida en la sección II de dicha Directiva, titulada «Criterios para la legitimación del tratamiento de datos», tenía el siguiente tenor:

«Los Estados miembros dispondrán que los datos personales sólo puedan tratarse si:

...

(f) el procesamiento es necesario para los fines de los intereses legítimos perseguidos por el controlador o por el tercero o terceros a quienes se revelan los datos, excepto cuando dichos intereses sean anulados por los intereses de los derechos y libertades fundamentales del interesado que requieren protección en virtud del artículo 1, apartado 1.».

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

«Los Estados miembros podrán adoptar medidas legislativas para restringir el alcance de las obligaciones y derechos previstos en el artículo 6, apartado 1, el artículo 10, el artículo 11, apartado 1, el artículo 12 y el artículo 21, cuando dicha restricción constituya una [medida] necesaria para salvaguardar:

...

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

– *El RGPD*

5 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; 'RGPD'), titulado 'Ámbito material', establece, en sus apartados 1 y 2:

'1. El presente Reglamento se aplica al tratamiento de datos personales total o parcialmente por medios automatizados y al tratamiento no automatizado de datos personales que forman parte de un fichero o están destinados a formar parte de un fichero.

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

...

d) por las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y prevención de amenazas a la seguridad pública.».

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

«A efectos del presente Reglamento:

(1) “datos personales” significa cualquier información relacionada con una persona física identificada o identificable (“titular de los datos”); …

(2) "procesamiento" significa cualquier operación o conjunto de operaciones que se realiza sobre datos personales o sobre conjuntos de datos personales, ya sea por medios automatizados o no, tales como recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación. , consulta, uso, divulgación por transmisión, difusión o puesta a disposición de otro modo, alineación o combinación, restricción, borrado o destrucción;

…'

7 El artículo 6 de dicho Reglamento, titulado «Legalidad del tratamiento», dispone en su apartado 1:

«El tratamiento sólo será lícito si y en la medida en que se aplique al menos una de las condiciones siguientes:

…

(f) el procesamiento es necesario para los fines de los intereses legítimos perseguidos por el controlador o por un tercero, excepto cuando dichos intereses sean anulados por los intereses o derechos y libertades fundamentales del interesado que requieren protección de datos personales…

El párrafo primero, letra f), no se aplicará al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.»

8 El artículo 9 de dicho Reglamento, titulado «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 revelen, en particular, datos relativos a la vida sexual o a la orientación sexual de una persona física no se aplica cuando el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos o es necesario, entre otras cosas, para el establecimiento, el ejercicio o la defensa de reclamaciones legales.

9 El artículo 23 del RGPD, titulado «Restricciones», dispone en su apartado 1:

«El Derecho de la Unión o de los Estados miembros al que esté sujeto el responsable o el encargado del tratamiento podrá restringir mediante medida legislativa el alcance de las obligaciones y derechos previstos en los artículos 12 a 22 y en el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones corresponden a los derechos y obligaciones previstos en los artículos 12 a 22, cuando tal restricción respeta la esencia de los derechos y libertades fundamentales y es 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 reclamaciones de Derecho civil.».

Normas sectoriales relativas a la protección de datos personales

– *Directiva 2002/58*

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

«(2) La presente Directiva pretende respetar los derechos fundamentales y observa los principios reconocidos, en particular, por [la Carta]. En particular, esta Directiva pretende garantizar el pleno respeto de los derechos establecidos en los artículos 7 y 8 de dicha Carta.

...

(6) Internet está trastornando las estructuras tradicionales del mercado al proporcionar una infraestructura global común para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles públicamente a través de Internet abren nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su privacidad.

(7) En el caso de las redes públicas de comunicaciones, deben adoptarse disposiciones jurídicas, reglamentarias y técnicas específicas para proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular en lo que respecta a la creciente capacidad de almacenamiento automatizado. y tratamiento de datos relativos a suscriptores y usuarios.

...

(11) Al igual que la Directiva [95/46], la presente Directiva no aborda cuestiones de protección de los derechos y libertades fundamentales relacionados con actividades que no se rigen por el Derecho comunitario. Por lo tanto, no altera el equilibrio existente entre el derecho del individuo a la privacidad y la posibilidad de que los Estados miembros adopten las medidas contempladas en el artículo 15, apartado 1, de la presente Directiva, necesarias para la protección de la seguridad pública, la defensa y la seguridad del Estado (incluidas el bienestar económico del Estado cuando las actividades se relacionan con cuestiones 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 llevar a cabo interceptaciones legales de comunicaciones electrónicas, o adoptar otras medidas, si fuera necesario para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales [firmado en Roma el 4 de noviembre de 1950], tal como lo interpretan las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deben ser apropiadas, estrictamente proporcionadas al fin previsto y necesarias en una sociedad democrática y deben estar sujetas 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 tratados en las redes de comunicaciones electrónicas para establecer conexiones y transmitir información contienen información sobre la vida privada de las personas físicas y se refieren al derecho al respeto de su correspondencia o a los intereses legítimos de las personas jurídicas. Dichos datos sólo podrán almacenarse en la medida necesaria para la prestación del servicio a efectos de facturación y pagos de interconexión, y durante un tiempo limitado. Cualquier procesamiento posterior de dichos datos... solo podrá permitirse si el suscriptor ha aceptado esto sobre la base de información precisa y completa proporcionada por el proveedor de los servicios de comunicaciones electrónicas disponibles públicamente sobre los tipos de procesamiento adicional que pretende realizar y sobre el el derecho del suscriptor a no dar o retirar su consentimiento para dicho procesamiento. ...

...

(30) Los sistemas para la prestación de redes y servicios de comunicaciones electrónicas deben diseñarse de modo que limiten al mínimo estricto la cantidad de datos personales necesarios. ...'

11 El artículo 2 de la Directiva 2002/58, titulado «Definiciones», dispone:

'...

También se aplicarán las siguientes definiciones:

(a) “usuario” significa cualquier persona física que utilice un servicio de comunicaciones electrónicas disponible públicamente, con fines privados o comerciales, sin necesariamente haberse suscrito a este servicio;

(b) “datos de tráfico” significa cualquier dato procesado con el fin de transmitir una comunicación en una red de comunicaciones electrónicas o para la facturación de la misma;

(c) “datos de ubicación” significa cualquier dato procesado 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 públicamente;

...'

12 El artículo 3 de dicha Directiva, titulado «Servicios de que se trata», 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 redes públicas de comunicaciones de la Comunidad, incluidas las redes públicas de comunicaciones que soportan dispositivos de identificación y recogida de datos".

13 El artículo 5 de la Directiva, titulado «Confidencialidad de las comunicaciones», dispone:

'1. Los Estados miembros garantizarán la confidencialidad de las comunicaciones y los datos de tráfico relacionados mediante una red pública de comunicaciones y servicios de comunicaciones electrónicas disponibles al público, a través de la legislación nacional. En particular, prohibirán la escucha, escucha, almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones y de los datos de tráfico relacionados por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, excepto cuando estén legalmente autorizados para ello de conformidad con el artículo 15(1). Este apartado no impedirá el almacenamiento técnico necesario para la transmisión de una comunicación sin perjuicio del principio de confidencialidad.

...

(3) Los Estados miembros garantizarán que el almacenamiento de información o el acceso a información ya almacenada en el equipo terminal de un abonado o usuario sólo esté permitido si el abonado o usuario en cuestión ha dado su consentimiento. haber recibido información clara y completa, de conformidad con la Directiva [95/46], entre otras cosas, sobre los fines del tratamiento. ...'

14 El artículo 6 de la Directiva 2002/58, titulado «Datos de tráfico», dispone:

'1. Los datos de tráfico relativos a abonados y usuarios tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán borrarse o anonimizarse cuando ya no sean necesarios para la transmisión de una comunicación, sin perjuicio de lo dispuesto en el apartado 2. , 3 y 5 del presente artículo y el artículo 15, apartado 1.

2. Podrán tratarse datos de tráfico necesarios a efectos de facturación de abonados y pagos de interconexión. Tal procesamiento sólo está permitido hasta el final del período durante el cual la factura puede ser legalmente impugnada o el pago.

3. Con el fin de comercializar servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido, el proveedor de un servicio de comunicaciones electrónicas disponible al público podrá tratar los datos a que se refiere el apartado 1 en la medida y durante el tiempo necesarios para dichos servicios o marketing. , si el suscriptor o usuario al que se refieren los datos ha dado su consentimiento previo. Los usuarios o suscriptores tendrán la posibilidad de retirar en cualquier momento su consentimiento para el tratamiento de datos de tráfico.

...

5. El tratamiento de datos de tráfico, de conformidad con los apartados 1, 2, 3 y 4, deberá limitarse a personas que actúen bajo la autoridad de proveedores de redes públicas de comunicaciones y servicios de comunicaciones electrónicas disponibles públicamente que se ocupen de la facturación o la gestión del tráfico, de las consultas de los clientes, detección de fraudes, comercialización de servicios de comunicaciones electrónicas o prestación de un servicio de valor añadido, debiendo limitarse a lo necesario para los fines de tales actividades.»

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

'1. Los Estados miembros podrán adoptar medidas legislativas para restringir el alcance de los derechos y obligaciones previstos en el artículo 5, el artículo 6, el artículo 8, apartados 1, 2, 3 y 4, y el artículo 9 de la presente Directiva cuando tales la restricción constituye una medida necesaria, apropiada y proporcionada dentro de una sociedad democrática para salvaguardar la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública y la prevención, investigación, detección y enjuiciamiento de delitos o del uso no autorizado del sistema de comunicación electrónica, tal como se contempla en el artículo 13, apartado 1, de la Directiva [95/46]. A tal fin, los Estados miembros podrán, entre otras cosas, adoptar medidas legislativas que prevean la conservación de datos durante un período limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas a que se refiere el presente apartado se ajustarán a los principios generales del Derecho comunitario, incluidos los contemplados en el artículo 6, apartados 1 y 2, [TUE].

...

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

...'

– *Directiva (UE) 2016/680*

16 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 las autoridades competentes con fines de prevención, investigación, detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y sobre 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), titulada «Objeto y objetivos», dispone, 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 datos personales por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la salvaguardia contra y la prevención de amenazas a la seguridad pública.'

17 El artículo 3 de dicha Directiva, titulado «Definiciones», dispone:

«A efectos de la presente Directiva:

...

(7) “autoridad competente” significa:

a) cualquier autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, incluida la protección y prevención de amenazas a la seguridad pública; o

b) cualquier otro organismo o entidad al que la legislación de los Estados miembros haya encomendado el ejercicio de poderes públicos y poderes públicos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la salvaguardia y la prevención de amenazas a la seguridad pública;

...'

Normas relativas a la protección de la propiedad intelectual.

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

'1. Los Estados miembros garantizarán que, en el marco de procedimientos relativos a una infracción de un derecho de propiedad intelectual y en respuesta a una solicitud justificada y proporcionada del demandante, las autoridades judiciales competentes puedan ordenar que se proporcione información sobre el origen y las redes de distribución de los bienes o servicios que infrinjan un derecho de propiedad intelectual sean prestados por el infractor...:

2. La información a que se refiere el apartado 1 comprenderá, según proceda:

(a) los nombres y direcciones de los productores, fabricantes, distribuidores, proveedores y otros poseedores anteriores de los bienes o servicios, así como de los mayoristas y minoristas previstos;

...

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

(a) otorgar al titular del derecho el derecho a recibir información más completa;

(b) regir el uso en procedimientos civiles o penales de la información comunicada de conformidad con este Artículo;

(c) regular la responsabilidad por el mal uso del derecho de información; o

(d) brindar una oportunidad para negarse a proporcionar información que obligaría a la persona mencionada en el párrafo 1 a admitir su propia participación o la de sus parientes cercanos en una infracción de un derecho de propiedad intelectual; o

e) regularán la protección de la confidencialidad de las fuentes de información o del tratamiento de datos personales.»

ley francesa

El IPC

19 El artículo L. 331-12 del Código de la Propiedad Intelectual, en su versión vigente en la fecha de la decisión impugnada por los 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; "Hadopi")] es una autoridad pública independiente. ...'

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

'[Hadopi] deberá:

1. Fomentar el desarrollo de ofertas legales y controlar el uso lícito e ilícito de obras y prestaciones cubiertas por un derecho de autor o un derecho conexo en las redes de comunicaciones electrónicas utilizadas para la prestación de servicios públicos de comunicación en línea;

2. Proteger dichas obras y prestaciones de las infracciones de aquellos derechos cometidas en las redes de comunicaciones electrónicas utilizadas para la prestación de servicios públicos de comunicaciones en línea;

...'

21 Según el artículo L. 331-15 de dicho Código:

«[Hadopi] estará compuesto por un Colegio y un Comité de protección de los derechos. ...

...

En el ejercicio de sus funciones, los miembros del Colegio y del Comité de protección de derechos no recibirán instrucciones de autoridad alguna.»

22 El artículo L. 331-17, párrafo primero, de dicho Código dispone:

«El Comité de protección de los derechos será el encargado de adoptar las medidas previstas en el artículo L. 331-25.»

23 Según el artículo L. 331-21 del IPC:

«Para que el Comité de protección de los derechos pueda desempeñar sus funciones, [Hadopi] estará compuesto por funcionarios públicos jurados autorizados por [su] Presidente, en las condiciones fijadas por decreto dictado previa audiencia al Consejo de Estado [(Consejo de Estado, Francia)]. ...

Los miembros del Comité de protección de los derechos y los funcionarios mencionados en el párrafo anterior serán remitidos al Comité en la forma prevista en el artículo L. 331-24. Examinarán los hechos.

Podrán, cuando sea necesario a efectos del procedimiento, obtener cualquier documento, independientemente del soporte en el que esté almacenado, incluidos los datos que hayan sido conservados y tratados por los operadores de comunicaciones electrónicas en virtud del artículo L. 34-1 del código de postes et des Communications Électroniques [(Código Postal y de Comunicaciones Electrónicas)] y por los proveedores de servicios mencionados en el artículo 6, apartado I, puntos 1 y 2, de la Ley nº 2004-575 de 21 de junio de 2004 para la confianza en la economía. numérique [(Ley nº 2004-575, de 21 de junio de 2004, de fomento de la confianza en la economía digital)].

También podrán obtener copias de los documentos mencionados en el párrafo anterior.

Podrán, en particular, obtener de los operadores de comunicaciones electrónicas la identidad, dirección postal, dirección de correo electrónico y número de teléfono del suscriptor cuyo acceso a los servicios públicos de comunicaciones en línea haya sido utilizado a los efectos de la reproducción, representación, puesta a disposición o comunicación al público de obras o prestaciones protegidas sin la autorización de los titulares de los derechos... cuando dicha autorización sea necesaria.»

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

«El Comité de protección de los derechos actuará previa propuesta de agentes jurados y autorizados... designados por:

– órganos profesionales de defensa legalmente constituidos;

– organizaciones de gestión colectiva;

– el Centre national du cinéma et de l'image animée [(Centro Nacional del Cine y de la Imagen en Movimiento, Francia)].

El Comité para la protección de los derechos también podrá actuar basándose en la información que le transmita el procurador de la República [(Fiscalía, Francia)].

No se le podrán imputar conductas delictivas que se remontan a más de seis meses.'

25 Según el artículo L. 331-25 de dicho Código, que regula el procedimiento de "respuesta gradual":

«Cuando el comportamiento infractor al que se refiere pueda constituir un incumplimiento de la obligación prevista en el artículo L. 336-3 [del CPI], el Comité para la protección de los derechos podrá enviar al abonado... una recomendación en la que su atención a las disposiciones del artículo L. 336-3, condenándole a cumplir la obligación prevista en dichas disposiciones y advirtiéndole de las sanciones que pueden imponerse en aplicación de los artículos L. 335-7 y L. 335. -7-1. Esta recomendación también proporcionará información al abonado sobre los contenidos culturales disponibles legalmente en línea, la existencia de medidas de seguridad para evitar el incumplimiento de la obligación prevista en el artículo L. 336-3 y los riesgos para el crecimiento de la producción artística y para la economía. de la industria cultural planteadas por prácticas que no respetan los derechos de autor y derechos afines.

Si el abonado vuelve a incurrir en un comportamiento que pueda constituir un incumplimiento de la obligación prevista en el artículo L. 336-3 dentro de los seis meses siguientes al envío de la recomendación mencionada en el párrafo primero, el Comité podrá emitir una nueva recomendación por medios electrónicos. que contenga la misma información que la recomendación anterior... Debe adjuntar a esa recomendación una carta entregada con acuse de recibo firmado o cualquier otro medio capaz de acreditar la fecha de entrega de esa recomendación.

Las recomendaciones formuladas en virtud del presente artículo indicarán la fecha y la hora en que se haya detectado la conducta que pueda constituir un incumplimiento de la obligación prevista en el artículo L. 336-3. Sin embargo, no divulgarán el contenido de las obras protegidas ni de la materia afectada por ese incumplimiento. Indicarán el número de teléfono, la dirección postal y la dirección de correo electrónico a los que el destinatario de la recomendación podrá dirigir, si así lo desea, sus observaciones al Comité de protección de derechos y obtendrá, previa solicitud expresa, datos de el contenido de las obras protegidas o de las prestaciones afectadas por la falta denunciada.»

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

«[Hadopi] está autorizada a establecer un sistema para el tratamiento automatizado de datos personales relativos a personas físicas que sean objeto de un procedimiento en virtud del presente inciso.

La finalidad de dicho tratamiento será permitir al Comité de protección de derechos implementar las medidas previstas en este inciso, realizar cuantos actos procesales conexos y aplicar los procedimientos para informar a los órganos profesionales de defensa y a las entidades de gestión colectiva de cualquier remisiones a una autoridad judicial y de las notificaciones a que se refiere el párrafo quinto del artículo L. 335-7.

Las normas detalladas para la aplicación del presente artículo se establecerán mediante decreto... Dichas normas establecerán, entre otras cosas:

– las categorías de datos que pueden registrarse y el período de tiempo durante el cual pueden conservarse;

– los sujetos a los que se podrán comunicar dichos datos, entre los que se incluirán los proveedores de acceso a servicios públicos de comunicación en línea;

– la manera en que los interesados pueden ejercer, ante [Hadopi], su derecho de acceso a los datos que les conciernen...»

27 Los párrafos primero y segundo del artículo L. 335-2 de dicho Código establecen:

'Toda edición de escritos, composiciones musicales, dibujos, pinturas o cualquier otra producción, impresa o grabada total o parcialmente, contraria a las leyes y reglamentos relativos a la propiedad de los autores, es una falsificación y toda falsificación constituye un delito.

La falsificación en Francia de obras publicadas en Francia o en el extranjero se castiga con tres años de prisión y una multa de 300.000 euros.»

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

«Toda fijación, reproducción, comunicación o puesta a disposición del público, a título oneroso o gratuito, o toda emisión televisiva de una interpretación, fonograma, videograma, programa o publicación de prensa, realizada sin la autorización, en su caso, del artista intérprete o ejecutante. , el productor de fonogramas o videogramas, la empresa de comunicación audiovisual, el editor de prensa o la agencia de noticias será castigado con tres años de prisión y una multa de 300.000 euros.»

29 El artículo L. 335-7 del CPI establece las normas relativas a la imposición, a los culpables de las infracciones penales contempladas, en particular, en los artículos L. 335-2 y L. 335-4 de dicho Código, de la pena adicional de suspensión del acceso a un servicio público de comunicación en línea por un período máximo de un año.

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

«En el caso de infracciones leves de la quinta clase previstas en el presente Código, cuando así lo establezca la reglamentación, podrá imponerse, según las mismas reglas, la pena suplementaria definida en el artículo L. 335-7, en caso de infracción grave. negligencia, por parte del titular del acceso a un servicio público de comunicación en línea al que el Comité para la protección de los derechos, en virtud del artículo L. 331-25, haya enviado previamente, mediante carta entregada con acuse de recibo firmado o por cualquier otro medio de acreditar la fecha de presentación, una recomendación en la que se le pide que adopte medidas que garanticen su acceso a Internet.»

31 Según el artículo L. 336-3 de dicho Código:

«Quien tenga derecho a acceder a servicios públicos de comunicaciones en línea tendrá la obligación de garantizar que dicho acceso no se utilice con fines de reproducción, representación, puesta a disposición o comunicación al público de obras o prestaciones protegidas por derechos de autor o por un derecho conexo sin la autorización de sus titulares... cuando dicha autorización sea necesaria.

El incumplimiento por parte de la persona que tiene acceso de la obligación prevista en el párrafo primero no tendrá por efecto hacerle responsable penalmente...»

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

«Los operadores de comunicaciones electrónicas... y los proveedores de servicios... enviarán, mediante una conexión al sistema automatizado de tratamiento de datos personales mencionado en el artículo L. 331-29 o mediante 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° 2010-236] en un plazo de ocho días a partir de la recepción del Comité de protección de derechos los datos técnicos necesarios para identificar al abonado cuyo acceso a los servicios públicos de comunicaciones en línea se ha utilizado para los fines de la reproducción, representación, puesta a

disposición o comunicación al público de obras o prestaciones protegidas sin la autorización de los titulares de los derechos... cuando dicha autorización sea necesaria.»

33 Según el artículo R. 331-40 de dicho Código:

«Cuando, en el plazo de un año a partir de la presentación de la recomendación mencionada en el párrafo primero del artículo L. 335-7-1, se señalen nuevas conductas infractoras que puedan constituir negligencia grave, tal como se definen en el artículo R. 335-5 del Comité de protección de derechos, informará al suscriptor, mediante carta entregada con acuse de recibo firmado, que podrá ser procesado por esa conducta. Dicha carta invitará al interesado a presentar sus observaciones en un plazo de quince días. Indicará que podrá, en el mismo plazo, solicitar una audiencia con arreglo al artículo L. 331-21-1 y que tiene derecho a representación letrada. También invitará al interesado a especificar sus responsabilidades y recursos familiares.

El Comité para la protección de los derechos podrá, por propia iniciativa, invitar al interesado a asistir a una audiencia. En la carta de invitación se indicará que el interesado tiene derecho a ser asistido por un abogado.»

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

'I. – Cuando se cumplan las condiciones previstas en el apartado II, comete negligencia grave, sancionable con la multa prevista para las infracciones leves de quinta clase, la que comete quien tenga derecho a acceder a servicios públicos de comunicaciones en línea y que, sin motivo legítimo, :

1. no ha establecido medidas para hacer seguro dicho acceso; o

2. no ha ejercido el debido cuidado en la implementación de dichas medidas.

II. – Lo dispuesto en el apartado I no se aplicará salvo que se cumplan las dos condiciones siguientes:

1. En virtud del artículo L. 331-25 y de conformidad con las exigencias formales previstas en dicho artículo, el Comité para la protección de los derechos ha recomendado a la persona que tiene derecho de visita que adopte medidas para garantizar su acceso de manera que para impedir que dicho acceso sea utilizado nuevamente con fines de reproducción, representación, puesta a disposición o comunicación al público de obras o prestaciones protegidas por derechos de autor o por un derecho conexo sin la autorización de los titulares de esos derechos... cuando dicha autorización se requiere;

2. Durante el año siguiente a la recepción de dicha recomendación, dicho acceso se utilizará de nuevo para los fines previstos en el punto 1 del apartado II.»

35 Con efecto a partir del 1 de enero de 2022, de conformidad con la ley n.º 2021-1382 , del 25 de octubre de 2021, relativa a la régulation et à la Protection de l'accès aux œuvres culturelles à l'ère numérique [(Ley n.º 2021-1382 de 25 de octubre de 2021 sobre la regulación y protección del acceso a las obras culturales en la era digital)] (JORF n.º 250 de 26 de octubre de 2021, texto n.º 2), Hadopi se fusionó con el Conseil supérieur de l'audiovisuel (CSA) [(Superior Consejo del sector audiovisual (CSA), Francia)], otra autoridad pública independiente, para formar la Autorité de régulation de lacommunication audiovisuelle et numérique (ARCOM) [(Autoridad para la Regulación de las Comunicaciones Audiovisuales y Digitales (ARCOM), Francia)].

36 Sin embargo, el procedimiento de respuesta escalonada, mencionado en el apartado 25 supra, se ha mantenido esencialmente inalterado, aunque ya no lo aplica el Comité de protección de los derechos de Hadopi, que estaba compuesto por tres miembros designados por el Consejo de Estado (Consejo de Estado), la Cour des comptes (Tribunal de Cuentas, Francia) y la Cour de cassation (Tribunal de Casación, Francia), respectivamente, sino por dos miembros del consejo de administración de ARCOM, uno de los cuales es designado por el Conseil d 'État (Consejo de Estado) y el otro por la Cour de cassation (Tribunal de Casación).

Decreto N° 2010-236

37 El artículo 1 del Decreto nº 2010-236, adoptado sobre la base, en particular, del artículo L. 331-29 del IPC, dispone:

'El sistema de tratamiento de datos personales denominado "Sistema de gestión de medidas de protección de obras en Internet" tiene por objeto permitir a la Comisión de protección de los derechos de [Hadopi]:

1. aplicar las medidas previstas en el Libro III de la parte legislativa del [CPI] (Título III, Capítulo I, Sección 3, Inciso 3) y en el Libro III de la parte reglamentaria de dicho código (Título III, Capítulo I, Sección 2, Subsección 2);

2. remitir al Ministerio Público las conductas que puedan constituir delito en virtud de los artículos L. 335-2, L. 335-3, L. 335-4 y R. 335-5 del [CPI] e informar órganos profesionales de defensa y organismos de gestión colectiva de dichas remisiones;

...'

38 El artículo 4 de dicho Decreto dispone:

'I. – Los funcionarios públicos jurados autorizados por el Presidente de [Hadopi] en virtud del artículo L. 331-21 del [CPI] y los miembros del Comité para la protección de los derechos mencionados en el artículo 1 tendrán acceso directo a los datos personales y información a que se refiere el anexo del presente Decreto.

II – A los operadores de comunicaciones electrónicas y a los proveedores a que se refiere el punto 2 del Anexo de este Decreto se les enviará:

– los datos técnicos necesarios para identificar al abonado;

– las recomendaciones previstas en el artículo L. 331-25 del [CPI] para la notificación por medios electrónicos a sus suscriptores;

– la información necesaria para la implementación de sanciones adicionales de suspensión de acceso a un servicio público de comunicaciones en línea notificadas a la Comisión de Protección de Derechos por el Ministerio Público.

III – Las remisiones al Ministerio Público serán informadas a los órganos profesionales de defensa y a las organizaciones de gestión colectiva.

IV – Se enviarán a las autoridades judiciales los informes sobre conductas susceptibles de constituir delito en virtud de 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 [IPC].

La ejecución de una pena de suspensión se notificará al sistema automatizado de antecedentes penales.»

39 El anexo de dicho Decreto dispone:

«Los datos e información personal registrados en el sistema de tratamiento denominado "Sistema de gestión de medidas de protección de obras en Internet" serán los siguientes:

1. Datos personales e información de los órganos de defensa profesional legalmente constituidos, de las entidades de gestión colectiva, del Centro Nacional del Cine y la Imagen en Movimiento y del Ministerio Público:

Respecto de los comportamientos que pueden constituir un incumplimiento de la obligación prevista en el artículo L. 336-3 del [CPI]:

Fecha y hora del suceso;

Dirección IP de los suscriptores interesados;

Se utiliza el protocolo peer-to-peer;

Seudónimo utilizado por el suscriptor;

Información sobre las obras protegidas o materia afectada por la conducta;

Nombre del archivo tal como aparece en el dispositivo del suscriptor (cuando corresponda);

Proveedor de servicios de Internet a través del cual se organizó el acceso o que suministró el recurso técnico IP.

...

2. Datos personales e información relativa al abonado recopilados de los operadores de comunicaciones electrónicas... y proveedores...:

Apellidos, nombres;

Dirección postal y direcciones de correo electrónico;

Número de teléfono;

Dirección de la instalación telefónica del abonado;

proveedor de servicios de Internet, utilizando las instalaciones técnicas del proveedor de servicios mencionado en el punto 1 con el que el abonado haya celebrado un contrato; número de referencia;

Fecha de inicio de la suspensión del acceso a un servicio público de comunicaciones en línea.

...'

El Código Postal y de Comunicaciones Electrónicas

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

«Los operadores de comunicaciones electrónicas conservarán:

1. a efectos de actuaciones penales, prevención de amenazas a la seguridad pública y salvaguardia de la seguridad nacional, la información relativa a la identidad civil del usuario hasta el vencimiento de un plazo de cinco años a partir de la fecha de finalización de su contrato;

2. para los mismos fines que los establecidos en el apartado II *bis* (1), otra información proporcionada por el usuario al celebrar un contrato o crear una cuenta y la información de pago hasta la expiración de un período de un año a partir de la fecha en que su contrato finaliza o su cuenta es cerrada;

3. A efectos de combatir delitos graves, prevenir amenazas graves para la seguridad pública y salvaguardar la seguridad nacional, los datos técnicos que permitan identificar la fuente de conexión o relativos al equipo terminal utilizado hasta la expiración de un período de un año desde la conexión. o utilización del equipo terminal.».

El litigio principal y las cuestiones prejudiciales

41 Al haber rechazado implícitamente el Premier ministre (Primer Ministro, Francia) su solicitud de derogación del Decreto nº 2010-236, los demandantes en el litigio principal interpusieron un recurso ante el Conseil d'État (Consejo de Estado), a instancia de 12 agosto de 2019, solicitando la anulación de esa decisión de rechazo implícito. Alegan, en esencia, que los párrafos tercero a quinto del artículo L. 331-21 del CPI, que forma parte de la base jurídica de dicho Decreto, (i) son contrarios al derecho al respeto de la vida privada consagrado en el Constitución francesa y (ii) infringe el Derecho de la UE, en particular el artículo 15 de la Directiva 2002/58 y los artículos 7, 8, 11 y 52 de la Carta.

42 En lo que respecta a la parte del recurso relativa a la supuesta violación de la Constitución, el Conseil d'État (Consejo de Estado) planteó una cuestión prioritaria de constitucionalidad al Conseil constitutionnel (Consejo Constitucional, Francia).

43 Mediante Decisión n.º 2020-841 QPC, de 20 de mayo de 2020, La Quadrature du Net et autres [Derecho de comunicación a la Hadopi], el Conseil constitutionnel (Consejo Constitucional) declaró los párrafos tercero y cuarto del artículo L. 331-21 del CPI es contrario a la Constitución, pero declaró que el quinto párrafo de ese artículo –con excepción de las palabras "en particular"- era compatible con la Constitución.

44 En lo que respecta a la parte del recurso relativa a la supuesta infracción del Derecho de la Unión, los demandantes en el litigio principal alegaron, en particular, que el Decreto nº 2010-236 y las disposiciones que constituyen su base jurídica permiten el acceso a los datos de conexión de forma desproporcionada. de manera penal por infracciones no graves de derechos de autor cometidas en Internet, sin revisión previa de un juez o de una autoridad que ofrezca garantías de independencia e imparcialidad. En particular, dichas infracciones no entran en el ámbito de los «delito grave» tal como se contempla en 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 órgano jurisdiccional remitente, el Conseil d'État (Consejo de Estado), señala, en primer lugar, 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 consideró, en particular, que el artículo 15, apartado 1, de la Directiva 2002/58, leído a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, no se opone a medidas legislativas que, a efectos de salvaguardar la

seguridad nacional, luchar contra la delincuencia y salvaguardar la seguridad pública, prevean la conservación general e indiscriminada de datos relativos a la identidad civil de los usuarios de sistemas de comunicaciones electrónicas. . En consecuencia, cuando se trate de datos relativos a la identidad civil de los usuarios de sistemas de comunicaciones electrónicas, dicha conservación está permitida, sin que se imponga ningún límite temporal específico, a los efectos de la investigación, detección y persecución de delitos en general. La Directiva 2002/58 tampoco se opone al acceso a dichos datos para tales fines.

46 El órgano jurisdiccional remitente deduce de ello que, en lo que respecta al acceso a los datos relativos a la identidad civil de los usuarios de sistemas de comunicaciones electrónicas, el motivo invocado por los demandantes en el litigio principal, basado en la ilegalidad del Decreto nº 2010-236, ya que fue adoptado en Debe rechazarse el contexto de actuación para luchar contra las infracciones no graves.

47 El órgano jurisdiccional remitente señala, en segundo lugar, que en 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, entre otras cosas, que entre otras cosas, que el artículo 15, apartado 1, de la Directiva 2002/58, leído a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una legislación nacional que regula la protección y la seguridad del tráfico y datos de localización y, en particular, el acceso de las autoridades nacionales competentes a los datos conservados, cuando ese acceso no esté sujeto a un control previo por parte de un tribunal o de un organismo administrativo independiente.

48 El órgano jurisdiccional remitente se remite, más concretamente, al apartado 120 de dicha sentencia, en el que el Tribunal de Justicia afirmó que es esencial que dicho acceso a los datos conservados esté, por regla general, salvo en casos de urgencia debidamente justificada, sujeto a la exigencia de un control previo llevado a cabo por un tribunal o por un organismo administrativo independiente, y que la decisión de ese tribunal u organismo debe adoptarse previa solicitud motivada de dichas autoridades presentada, entre otros, en el marco de los procedimientos de prevención , detección o persecución del delito.

49 El Tribunal de Justicia se refirió a 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), como en lo que respecta a la recogida en tiempo real de datos de conexión por parte de 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 que respecta al acceso de las autoridades nacionales a los datos de conexión.

50 El tribunal remitente señala también que Hadopi, desde su creación en 2009, ha emitido más de 12,7 millones de recomendaciones a sus suscriptores en el marco del procedimiento de respuesta gradual previsto en el artículo L. 331-25 del IPC, de las cuales 827.791 sólo en 2019. De ello se deduce que los funcionarios del Comité para la protección de los derechos de Hadopi tuvieron necesariamente que recopilar, cada año, un volumen considerable de datos relativos a la identidad civil de los usuarios interesados. El órgano jurisdiccional remitente considera que, habida cuenta del volumen de dichas recomendaciones, someter dicha recopilación de datos a un control previo podría imposibilitar la emisión de 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 están incluidos entre los datos de tráfico y de localización a los que, en principio, se aplica la exigencia de control previo por

parte de un tribunal o de una entidad administrativa independiente [cuyas decisiones son vinculantes]?

(2) En caso de respuesta afirmativa a la primera cuestión, y teniendo en cuenta que los datos relativos a la identidad civil de los usuarios, incluidos sus datos de contacto, no son datos especialmente sensibles, debe leerse la Directiva [2002/58]. a la luz de la [Carta], debe interpretarse en el sentido de que se opone a la legislación nacional que prevé la recopilación de esos datos, correspondientes a las direcciones IP de los usuarios, por una autoridad administrativa, sin control previo por parte de un tribunal o de una entidad administrativa independiente [¿cuyas decisiones son vinculantes]?

(3) Si se responde afirmativamente a la segunda cuestión, y teniendo en cuenta que los datos relativos a la identidad civil no son datos especialmente sensibles, sólo podrán recogerse dichos datos y únicamente con el fin de prevenir incumplimientos de obligaciones definidas de forma precisa, exhaustiva y restrictiva por el Derecho nacional, y que el control sistemático del acceso a los datos de cada usuario por parte de un tribunal o de una tercera entidad administrativa [cuyas decisiones son vinculantes] podría causar poner en peligro el cumplimiento del servicio público confiado a la autoridad administrativa que recoge estos datos, que es ella misma independiente, no impide [la Directiva 2002/58] que el control se realice de forma adaptada, por ejemplo como un control automatizado, en su caso, bajo la supervisión de un servicio del organismo que ofrezca garantías de independencia e imparcialidad frente a los funcionarios encargados de recoger los datos?»

Examen de las cuestiones planteadas

52 Mediante sus tres cuestiones, que procede examinar conjuntamente, el órgano jurisdiccional remitente pregunta, en esencia, si el artículo 15, apartado 1, de la Directiva 2002/58, leído a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1,) de la Carta, debe interpretarse en el sentido de que se opone a una legislación nacional que autoriza a la autoridad pública responsable de la protección de los derechos de autor y derechos afines contra las infracciones de dichos derechos cometidas en Internet a acceder a datos conservados por proveedores de servicios de comunicaciones electrónicas disponibles al público, relacionados con a la identidad civil asociada a las direcciones IP previamente recopiladas por las organizaciones titulares de derechos, de modo que dicha autoridad pública pueda identificar a los titulares de dichas direcciones –que han sido utilizadas para actividades que pueden constituir tales infracciones– y pueda, en su caso, tomar medidas contra ellos, sin que dicho acceso esté sujeto al requisito de una revisión previa por parte de un tribunal o de un órgano administrativo independiente.

Observaciones preliminares

53 El asunto principal se refiere a dos tratamientos de datos personales separados y sucesivos realizados en el marco de las actividades de Hadopi, autoridad pública independiente cuya misión, de conformidad con el artículo L. 331-13 del CPI, es proteger obras y materias cubiertas por derechos de autor o derechos conexos contra las infracciones de esos derechos cometidas en las redes de comunicaciones electrónicas utilizadas para la prestación de servicios públicos de comunicación en línea.

54 La primera operación de procesamiento, realizada previamente por agentes autorizados y jurados de las organizaciones de titulares de derechos, se desarrolla en dos etapas. En primer lugar, las direcciones IP que parecen haber sido utilizadas para actividades que pueden constituir una infracción de los derechos de autor o derechos conexos se recopilan en redes peer-to-peer. En

segundo lugar, se pone a disposición de Hadopi un conjunto de datos e información personal en forma de informes. Estos datos son, según la lista que figura en el punto 1 del anexo del Decreto nº 2010-236, la fecha y la hora del suceso, la dirección IP de los abonados en cuestión, el protocolo peer-to-peer utilizado, el seudónimo utilizado por el suscriptor, información relacionada con las obras protegidas o la materia afectada por la conducta, el nombre del archivo tal como aparece en el dispositivo del suscriptor (si corresponde) y el proveedor de servicios de Internet a través del cual se organizó el acceso o que suministró el recurso técnico de IP.

55 La segunda operación de tratamiento, realizada posteriormente por los proveedores de servicios de Internet a petición de Hadopi, se desarrolla también en dos etapas. En primer lugar, las direcciones IP recopiladas en sentido ascendente se comparan con los titulares de esas direcciones. En segundo lugar, se pone a disposición de dicha autoridad pública un conjunto de datos e informaciones personales relativos a dichos titulares, que se refieren esencialmente a su identidad civil. Estos datos son, según la lista que figura en el punto 2 del anexo del Decreto no 2010-236, esencialmente, el apellido y el nombre del abonado, la dirección postal y de correo electrónico, el número de teléfono y la dirección de la instalación telefónica del abonado.

56 Respecto a este último, el artículo L. 331-21, párrafo quinto, del CPI, en su versión resultante de la decisión del Conseil constitutionnel mencionada en el apartado 43 supra, establece que los miembros del Comité de Hadopi para la protección de derechos y los funcionarios públicos jurados de dicha autoridad autorizados por su presidente podrán obtener de los operadores de comunicaciones electrónicas la identidad, dirección postal, dirección de correo electrónico y número de teléfono del suscriptor cuyo acceso a servicios públicos de comunicación en línea haya sido utilizado para fines de reproducción. , representación, puesta a disposición o comunicación al público de obras o prestaciones protegidas sin la autorización de los titulares de los derechos cuando dicha autorización sea requerida.

57 Estas diferentes operaciones de tratamiento de datos personales tienen por objeto permitir a Hadopi adoptar, respecto de los titulares de direcciones IP así identificados, las medidas previstas en el procedimiento administrativo denominado "respuesta gradual" regulado por el artículo L. 331-25 del IPC. Estas medidas son, en primer lugar, el envío de "recomendaciones", que son similares a advertencias; luego, en caso de remisión al comité de derechos de Hadopi, dentro del plazo de un año después del envío de una segunda recomendación, respecto de una conducta que pueda constituir una repetición de la conducta infractora detectada, la notificación al suscriptor, tal como se indica previsto en el artículo R. 331-40 del CPI, que la conducta puede constituir un delito de "negligencia grave", definido en el artículo R. 335-5 del CPI, infracción leve sancionable con una multa máxima de 1 euro. 500 y 3 000 euros en caso de reincidencia; y, por último, previa deliberación, la remisión al Ministerio Fiscal de conductas que puedan constituir una infracción leve o, en su caso, el delito de falsificación previsto en el artículo L. 335-2 del IPC o en el artículo L. 335-4 de dicho código, castigado con tres años de prisión y una multa de 300.000 euros.

58 Dicho esto, las cuestiones planteadas por el órgano jurisdiccional remitente se refieren únicamente al tratamiento posterior descrito en el apartado 55 supra y no al tratamiento previo, cuyas características esenciales fueron expuestas en el apartado 54 supra.

59 Sin embargo, hay que señalar que, si la recopilación previa de direcciones IP por parte de las organizaciones titulares de derechos en cuestión fuera contraria al Derecho de la UE, el Derecho de la UE también impediría el uso de esos datos en el contexto del tratamiento posterior por parte de proveedores de servicios de comunicaciones electrónicas que consisten en al cotejar dichas direcciones con los datos relativos a la identidad civil de los titulares de dichas direcciones.

60 En este contexto, procede recordar de entrada que, según la jurisprudencia del Tribunal de Justicia, las direcciones IP constituyen tanto datos de tráfico a efectos de la Directiva 2002/58 como datos personales a efectos del RGPD (véase, en su lugar, en efecto, sentencia de 17 de junio de 2021, *MICM* , C-597/19, EU:C:2021:492, apartados 102 y 113 y jurisprudencia citada).

61 Sin embargo, la recopilación de direcciones IP públicas y visibles para todos, por parte de agentes de organizaciones de titulares de derechos, no entra en el ámbito de aplicación de la Directiva 2002/58, ya que dicho tratamiento claramente no tiene lugar «en relación con la prestación de [...] servicios de comunicaciones electrónicas», en el sentido del artículo 3 de dicha Directiva.

62 En cambio, tal recopilación de direcciones IP, autorizada, como se desprende de los autos, dentro de determinados límites cuantitativos y en determinadas condiciones, por la Commission nationale de l'informatique et des libertés (CNIL) (Comisión Nacional de Tecnologías de la Información y Libertades Civiles (CNIL), Francia), con vistas a su transmisión a Hadopi con el fin de su posible uso en procedimientos administrativos o judiciales posteriores destinados a combatir actividades que infrinjan los derechos de autor y derechos afines, constituye un "procesamiento" , en el sentido del artículo 4, apartado 2, del RGPD, cuya legalidad depende de las condiciones establecidas en el artículo 6, apartado 1, párrafo primero, letra f), de dicho Reglamento, a la luz del asunto del Tribunal de Justicia -ley establecida, en particular, en las sentencias de 17 de junio de 2021, *MICM* (C-597/19, EU:C:2021:492, apartados 102 y 103), y de 4 de julio de 2023, *Meta Platforms y otros (General condiciones de uso de una red social) (* C-252/21, EU:C:2023:537, apartados 106 a 112 y jurisprudencia citada).

63 El tratamiento posterior descrito en el apartado 55 supra está comprendido en el ámbito de aplicación de la Directiva 2002/58, ya que tiene lugar «en relación con la prestación de [...] servicios de comunicaciones electrónicas», en el sentido del artículo 3 de dicha Directiva, en la medida en que ya que los datos en cuestión se obtienen de proveedores de servicios de comunicaciones electrónicas de conformidad con el artículo L. 331-21 del IPC.

Si el acceso de una autoridad pública a datos relativos a la identidad civil asociada a una dirección IP conservados por proveedores de servicios de comunicaciones electrónicas con el fin de luchar contra los delitos de falsificación cometidos en línea puede justificarse con arreglo al artículo 15, apartado 1, de la Directiva 2002/58

64 A la vista de las anteriores observaciones preliminares, se plantea la cuestión de si, como pregunta el tribunal remitente, la limitación de los derechos fundamentales consagrados en los artículos 7, 8 y 11 de la Carta que supone el acceso por parte de una autoridad pública, como Hadopi, a datos relativos a la identidad civil asociada a una dirección IP que ya posee puede justificarse con arreglo al artículo 15, apartado 1, de la Directiva 2002/58.

65 El acceso a dichos datos personales solo podrá concederse en la medida en que hayan sido conservados de manera compatible 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 los datos electrónicos). comunicaciones)* , C-746/18, EU:C:2021:152, apartado 29).

Los requisitos relacionados con la retención de datos relacionados con la identidad civil y las direcciones IP asociadas 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 introducir excepciones a la obligación de principio, establecida en el artículo 5, apartado 1, de dicha Directiva, de garantizar la confidencialidad de los datos personales, y a las obligaciones correspondientes, a que se refiere, entre otros, los artículos 6 y 9 de dicha Directiva, cuando dicha restricción constituya

una medida necesaria, adecuada y proporcionada en una sociedad democrática para salvaguardar la seguridad nacional, la defensa y la seguridad pública, así como la prevención, investigación, detección y enjuiciamiento de infracciones penales o de utilización no autorizada del sistema de comunicación electrónica. A tal fin, los Estados miembros podrán, entre otras cosas, adoptar medidas legislativas que prevean la conservación de datos durante un período limitado justificado por uno de esos motivos. Dicho esto, la posibilidad de establecer excepciones a los derechos y obligaciones establecidos en los artículos 5, 6 y 9 de la Directiva 2002/58 no puede permitir la excepción a la obligación de principio de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos relacionados con las mismas y, en en particular, a que se convierta en norma la prohibición de conservación de dichos datos, explícitamente establecida en el artículo 5 de dicha Directiva (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 tanto, un acto legislativo adoptado con arreglo a dicha disposición debe corresponder, real y estrictamente, a uno de los objetivos mencionados en el apartado anterior: la lista de dichos objetivos establecida en la primera frase del artículo 15, apartado 1, de la Directiva 2002/58 es exhaustivo – y cumplir con los principios generales del derecho de la UE, incluido el principio de proporcionalidad, y los derechos fundamentales garantizados por la Carta. A este respecto, el Tribunal de Justicia ya ha declarado que la obligación impuesta a los proveedores de servicios de comunicaciones electrónicas por un Estado miembro mediante la legislación nacional de conservar datos de tráfico con el fin de ponerlos a disposición, en caso necesario, de las autoridades nacionales competentes plantea cuestiones relativas a la compatibilidad no sólo con los artículos 7 y 8 de la Carta, relativos a la protección de la vida privada y a la protección de datos personales, respectivamente, sino también con el artículo 11 de la Carta, relativo a la libertad de expresión (véase, a ese en efecto, 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, 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 en el artículo 7 de la Carta, como del derecho a la protección de los datos personales. garantizado en el artículo 8 de la misma, tal como se desprende de la jurisprudencia del Tribunal, así como la importancia del derecho a la libertad de expresión, toda vez que ese derecho fundamental, garantizado en el artículo 11 de la Carta, constituye uno de los fundamentos esenciales de una sociedad pluralista y democrática, y es uno de los valores en los que, según el artículo 2 TUE, se fundamenta la Unión (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, procede subrayar que la conservación de datos de tráfico y de localización constituye, en sí misma, por un lado, una excepción a la prohibición establecida en el artículo 5, apartado 1, de la Directiva 2002/58 de impedir que cualquier persona distinta del usuario almacenar esos datos y, por otro, una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de datos personales, consagrados en los artículos 7 y 8 de la Carta, con independencia de que la información en cuestión relativa a la vida privada sea sensible o si las personas interesadas han sufrido algún tipo de molestia a causa de dicha injerencia. También es irrelevante si los datos conservados han sido utilizados posteriormente o no, ya que el acceso a dichos datos constituye una injerencia propia en los derechos fundamentales a que se refiere el párrafo anterior, con independencia del uso posterior que se haga de esos datos (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 Dicho esto, en la medida en que el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros introducir determinadas medidas de excepción, como se ha señalado en el

apartado 66 supra, esa disposición refleja el hecho de que los derechos consagrados en los artículos 7, 8 y 11 de la Carta no son derechos absolutos, sino que deben considerarse en relación con su función en la sociedad. En efecto, como se desprende del artículo 52, apartado 1, de la Carta, esta disposición permite imponer limitaciones al ejercicio de esos derechos, siempre que dichas limitaciones estén previstas por la ley, respeten la esencia de esos derechos y que , respetando el principio de proporcionalidad, son necesarios y responden realmente a objetivos de interés general reconocidos por la Unión Europea o a la necesidad de proteger 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, procede señalar que, si bien formalmente Hadopi sólo está autorizada a acceder a los datos relativos a la identidad civil asociada a una dirección IP, dicho acceso presenta la particularidad de que, en primer lugar, exige a los proveedores de servicios de comunicaciones electrónicas de que se trate cotejar la dirección IP con los datos de identidad civil del titular de esa dirección. Por tanto, ese acceso presupone necesariamente que los proveedores dispongan de las direcciones IP, así como de los datos relativos a la identidad de los titulares de dichas direcciones.

72 Además, dicha autoridad pública solicita el acceso a esos datos con el único fin de identificar al titular de una dirección IP que ha sido utilizada para actividades susceptibles de vulnerar los derechos de autor o derechos afines, ya que ha puesto ilegalmente a disposición en la red obras protegidas. Internet para que otros lo descarguen. En estas circunstancias, debe considerarse que los datos relativos a la identidad civil están estrechamente vinculados tanto a la dirección IP como a la información que Hadopi posee sobre la obra puesta a disposición en Internet.

73 Este contexto particular no puede ignorarse al examinar la posible justificación de una medida que prevé la conservación de datos personales con arreglo al artículo 15, apartado 1, de la Directiva 2002/58, interpretada a la luz de los artículos 7, 8 y 11 de la Carta (véase , por analogía, TEDH, sentencia de 24 de abril de 2018, *Benedik c. Eslovenia* , CE:ECHR:2018:0424JUD006235714, § 109).

74 Por tanto, es 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, interpretado a la luz de los artículos 7, 8 y 11 de la Carta, que Es necesario examinar cualquier justificación de la injerencia en los derechos fundamentales consagrados en dichos artículos de la Carta que supone la conservación, por parte de proveedores de servicios de comunicaciones electrónicas disponibles al público, de datos a los que Hadopi tiene poder de acceso.

75 En este contexto, procede señalar que, según la jurisprudencia del Tribunal de Justicia, si bien, como se recuerda en el apartado 60 supra, las direcciones IP constituyen datos de tráfico en el sentido de la Directiva 2002/58, son distintas de otras categorías de tráfico. datos y datos de ubicación.

76 A este respecto, el Tribunal de Justicia ha declarado que las direcciones IP se generan independientemente de cualquier comunicación concreta y sirven principalmente para identificar, a través de proveedores de servicios de comunicaciones electrónicas, al propietario del equipo terminal desde el que se realiza una comunicación por Internet. Así, en relación con el correo electrónico y la telefonía por Internet, siempre que sólo se conserven las direcciones IP de la fuente de la comunicación y no las direcciones IP del destinatario de la comunicación, dichas direcciones no revelan, como tales, ninguna información sobre terceros. quienes estuvieron en contacto con la persona que realizó la comunicación. En esta medida, esta categoría de datos es menos sensible que otros 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, a pesar de haber constatado que las direcciones IP son menos sensibles cuando sirven exclusivamente para identificar al usuario de un servicio de comunicaciones electrónicas, el artículo 15, apartado 1, de la Directiva 2002/58 se opone a la conservación general e indiscriminada únicamente de las direcciones IP asignadas a la fuente de una conexión con fines distintos de la lucha contra delitos graves, la prevención de amenazas graves a la seguridad pública o la salvaguardia de la seguridad nacional. Sin embargo, para llegar a esta conclusión, el Tribunal de Justicia se basó expresamente en la gravedad de la vulneración de los derechos fundamentales consagrados en los artículos 7, 8 y 11 de la Carta que dicha conservación de direcciones IP puede implicar.

78 El Tribunal de Justicia consideró, en el apartado 153 de la misma sentencia, que, dado que las direcciones IP pueden, entre otras cosas, cuando se utilizan para «seguir el flujo de clics completo de un usuario de Internet» y, por tanto, su actividad en línea, permitir un «perfil detallado» del usuario, la conservación y el análisis de las direcciones IP necesarias para dicho seguimiento constituyen una grave injerencia en los derechos fundamentales del usuario de Internet consagrados en los artículos 7 y 8 de la Carta, que también pueden disuadir a los usuarios de Internet sistemas de comunicación ejerzan su libertad de expresión garantizada por el Artículo 11 de la Carta.

79 Sin embargo, cabe señalar que la conservación general e indiscriminada de un conjunto –incluso un conjunto amplio– de direcciones IP estáticas y dinámicas utilizadas por una persona en un período determinado no constituye necesariamente, en todos los casos, una interferencia grave con la derechos fundamentales garantizados por los artículos 7, 8 y 11 de la Carta.

80 A este respecto, en primer lugar, los asuntos que dieron lugar a la sentencia de 6 de octubre de 2020, *La Quadrature du Net y otros* (C-511/18, C-512/18 y C-520/18, EU:C :2020:791), se refería a la legislación nacional que implicaba la obligación de conservar un conjunto de datos necesarios para determinar la fecha, hora, duración y tipo de comunicación, identificar los equipos de comunicaciones utilizados y determinar la ubicación del equipo terminal y del comunicaciones, datos que incluían, entre otros, el nombre y dirección del usuario, los números de teléfono del llamante y de la persona llamada y la dirección IP para servicios de Internet. Además, en dos de esos asuntos, la normativa nacional controvertida parecía abarcar también datos relativos al transporte de comunicaciones electrónicas por redes, lo que permite también identificar la naturaleza de la información consultada en línea (véase, en este sentido, la sentencia 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 Por lo tanto, la conservación de direcciones IP en virtud de dicha legislación nacional era tal –habida cuenta de los demás datos que dichas normas exigían conservar y de la posibilidad de combinar esos diversos datos– que permitía extraer conclusiones precisas sobre la vida privada de la persona. personas cuyos datos estaban afectados y, en consecuencia, dar lugar a una injerencia grave en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, relativos a la protección de la vida privada y de los datos personales de dichas personas, y en el artículo 11 de dicha Carta, sobre su libertad de expresión.

82 Por el contrario, una obligación impuesta a los proveedores de servicios de comunicaciones electrónicas, mediante una medida legislativa con arreglo al artículo 15, apartado 1, de la Directiva 2002/58, de garantizar la conservación general e indiscriminada de direcciones IP puede, según sea el caso, estar justificada. por el objetivo de luchar contra las infracciones penales en general, cuando realmente se excluye que dicha retención pueda dar lugar a injerencias graves en la vida privada del interesado debido a la posibilidad de extraer conclusiones precisas sobre dicha persona, entre

otras cosas, vinculando dichas infracciones Direcciones IP con un conjunto de datos de tráfico o ubicación que también han sido conservados por esos proveedores.

83 En consecuencia, un Estado miembro que pretenda imponer a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar direcciones IP, de manera general e indiscriminada, para alcanzar un objetivo vinculado a la lucha contra las infracciones penales en general debe garantizar que las disposiciones para la la conservación de dichos datos puede garantizar que cualquier combinación de dichas direcciones IP con otros datos, conservados de conformidad con la Directiva 2002/58, que permita extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se conservan de este modo, está descartado.

84 Para excluir tal combinación de datos que permita extraer conclusiones precisas sobre la vida privada del interesado, el régimen de conservación debe referirse a la forma misma en que se estructura la conservación; En esencia, dicha conservación debe organizarse de manera que se garantice una separación realmente estricta de las diferentes categorías de datos conservados.

85 A este respecto, corresponde efectivamente al Estado miembro que pretende imponer a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar las direcciones IP, de manera general e indiscriminada, para alcanzar un objetivo vinculado a la lucha contra las infracciones penales en general, establecer en su legislación normas claras y precisas relativas a dichos regímenes de retención, que deben cumplir requisitos estrictos. Sin embargo, el Tribunal podrá proporcionar aclaraciones sobre dichas disposiciones.

86 En primer lugar, las normas nacionales mencionadas en el párrafo anterior deben garantizar que cada categoría de datos, incluidos los datos relativos a la identidad civil y a las direcciones IP, se mantenga completamente separada de las demás categorías de datos conservadas.

87 En segundo lugar, dichas normas deben garantizar que, desde un punto de vista técnico, la separación de las distintas categorías de datos conservados, en particular los datos relativos a la identidad civil, las direcciones IP, los distintos datos de tráfico distintos de las direcciones IP y la diversos datos de localización, es realmente hermético, mediante un sistema informático seguro y fiable.

88 En tercer lugar, en la medida en que dichas normas prevén la posibilidad de vincular las direcciones IP conservadas con la identidad civil del interesado, respetando las exigencias derivadas del artículo 15, apartado 1, de la Directiva 2002/58, en su interpretación A la luz de los artículos 7, 8 y 11 de la Carta, sólo deben permitir dicha vinculación mediante el uso de un proceso técnico eficaz que no menoscabe la eficacia de la separación hermética de esas categorías de datos.

89 En cuarto lugar, la fiabilidad de esta separación hermética debe estar sujeta a un control periódico por parte de una autoridad pública distinta de la que pretende obtener acceso a los datos personales conservados por los proveedores de servicios de comunicaciones electrónicas.

90 En la medida en que la legislación nacional aplicable establece requisitos tan estrictos en relación con las disposiciones para la conservación general e indiscriminada de direcciones IP y otros datos conservados por los proveedores de servicios de comunicaciones electrónicas, la interferencia resultante de dicha conservación de direcciones IP no puede, debido a la forma misma en que se estructura dicha retención, calificarse de «graves».

91 Cuando se introduce un marco legislativo de este tipo, las disposiciones para la conservación de direcciones IP así prescritas excluyen la posibilidad de que esos datos puedan combinarse con otros

datos conservados de conformidad con la Directiva 2002/58, lo que permite extraer conclusiones precisas sobre el carácter privado vida del interesado.

92 En consecuencia, en presencia de un marco legislativo que cumpla los requisitos establecidos en los apartados 86 a 89 anteriores, garantizando que ninguna combinación de datos permita sacar conclusiones precisas sobre la vida privada de las personas en cuestión, el artículo 15, apartado 1, de la Directiva 2002/58, interpretada 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 conservar direcciones IP, de manera general e indiscriminada, con el fin de luchar contra la delincuencia. delitos en general.

93 Por último, tal marco legislativo debe, 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, UE: C:2020:791), prevén un período de conservación limitado a lo estrictamente necesario y garantizan, mediante normas claras y precisas, que la conservación de los datos en cuestión esté sujeta al cumplimiento de las condiciones sustantivas y procesales aplicables y que las personas interesadas dispongan de salvaguardias efectivas contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de dichos datos.

94 Corresponde al órgano jurisdiccional remitente comprobar si la normativa nacional controvertida en el litigio principal cumple los requisitos mencionados en los apartados 85 a 93 anteriores.

Los requisitos que rodean el acceso a los datos relacionados con la identidad civil asociada con una dirección IP conservada por los proveedores de servicios de comunicaciones electrónicas.

95 De la jurisprudencia del Tribunal se desprende que, en el ámbito de la lucha contra las infracciones penales, sólo los objetivos de combatir delitos graves o prevenir amenazas graves a la seguridad pública pueden justificar una injerencia grave en los derechos fundamentales consagrados en los artículos 7 y 8. de la Carta implica que las autoridades públicas tengan acceso a un conjunto de datos de tráfico o de localización, que pueden proporcionar información sobre las comunicaciones realizadas por un usuario de un medio de comunicación electrónica o sobre la ubicación del equipo terminal que utiliza y que permiten sacar conclusiones precisas sobre la vida privada de las personas interesadas, y otros factores relacionados con la proporcionalidad de una solicitud de acceso, como la duración del período respecto del cual se solicita el acceso a dichos datos, no pueden tener el efecto de que el objetivo de prevenir, investigar, detectar y perseguir delitos penales en general pueda justificar dicho acceso (sentencia de 2 de marzo de 2021, *Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas)* , C-746/18, UE :C:2021:152, apartado 35).

96 Sin embargo, cuando la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta implica el acceso de una autoridad pública a datos relativos a la identidad civil conservados por proveedores de servicios de comunicaciones electrónicas, sin que dichos datos puedan asociarse con información sobre las comunicaciones realizadas, no es grave puesto que, en su conjunto, dichos datos no permiten sacar conclusiones precisas sobre la vida privada de las personas de que se trata, dicho acceso puede estar justificado por un objetivo de prevención, de investigación , detección y persecución de infracciones penales en general (véase, en este sentido, sentencia de 2 de octubre de 2018, *Ministerio Fiscal* , C-207/16, EU:C:2018:788, apartados 54, 57 y 60).

97 Procede añadir además que, según un principio establecido en reiterada jurisprudencia del Tribunal de Justicia, el acceso a los datos de tráfico y de localización sólo puede estar justificado con arreglo al artículo 15, apartado 1, de la Directiva 2002/58 por el objetivo de interés público para el que se Se ordenó a los proveedores de servicios de comunicaciones electrónicas que conservaran esos

datos, excepto cuando ese acceso esté justificado por un objetivo de interés público más importante. De este principio se desprende, en particular, que tal acceso no podrá concederse en ningún caso para combatir infracciones en general cuando la conservación de dichos datos esté justificada por el objetivo de combatir delitos graves o, a fortiori, por el objetivo de salvaguardar 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 Sin embargo, este objetivo de lucha contra las infracciones penales en general puede justificar la concesión de acceso a datos de tráfico y de localización que fueron almacenados y, por tanto, conservados en la medida y durante el tiempo necesarios para la comercialización, la facturación de los servicios y la aportación de valor. servicios añadidos, tal 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 caso de autos, en primer lugar, de la normativa nacional controvertida en el litigio principal se desprende que Hadopi no tiene acceso a un «conjunto de datos de tráfico o de localización», en el sentido de la jurisprudencia citada. en el apartado 95 supra, de modo que, en principio, no puede extraer conclusiones precisas sobre la vida privada de las personas interesadas. Un acceso que no permita extraer tales conclusiones no constituye una injerencia grave en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta.

100 Según dicha legislación y las explicaciones proporcionadas por el Gobierno francés al respecto, el acceso concedido a dicha autoridad pública está estrictamente limitado a determinados datos relativos a la identidad civil del titular de una dirección IP y está autorizado con el único fin de permitir la identificación del titular sospechoso de haber participado en una actividad que infringe los derechos de autor o derechos conexos al haber puesto ilegalmente a disposición de otros obras protegidas en Internet para su descarga. La finalidad de dicho acceso es la adopción, en su caso, de una de las medidas educativas o punitivas previstas en el marco del procedimiento de respuesta gradual respecto de dicho titular, a saber, el envío de una primera y una segunda recomendación y, a continuación, de una carta de notificación. que dicha actividad pueda constituir un delito leve de negligencia grave y, por último, la remisión del asunto al Ministerio Público para la persecución de ese delito leve o del delito de falsificación.

101 Esta legislación nacional también debe establecer normas claras y precisas capaces de garantizar que las direcciones IP conservadas de conformidad con la Directiva 2002/58 sólo puedan utilizarse para identificar a la persona a la que se ha asignado una determinada dirección IP, excluyendo al mismo tiempo cualquier uso que permita la vigilancia, a través de una o varias de dichas direcciones, de la actividad en línea de esa persona. Cuando una dirección IP se utilice con el único fin de identificar a su titular en el marco de un procedimiento administrativo específico que pueda dar lugar a un procedimiento penal contra el interesado y no con fines tales como, por ejemplo, identificar los contactos o la ubicación de dicho titular, el acceso a esa dirección con ese único fin se refiere a esa dirección como datos relativos a la identidad civil y no como datos de tráfico.

102 Además, del principio establecido en reiterada jurisprudencia recordada en el anterior apartado 97 se desprende que un acceso como el que disfruta Hadopi con arreglo a la normativa nacional controvertida en el litigio principal, puesto que persigue el objetivo de luchar contra las infracciones penales en general, sólo puede justificarse si se refiere a direcciones IP que deben conservar los proveedores de servicios de comunicaciones electrónicas a efectos de dicho objetivo y no a efectos de un objetivo más importante como el de la lucha contra la delincuencia grave, sin perjuicio, no obstante, de acceso justificado por tal objetivo de lucha contra las infracciones en general cuando se refiere a direcciones IP almacenadas y, por tanto, conservadas en las condiciones establecidas en el artículo 6 de la Directiva 2002/58.

103 Además, como se desprende de los apartados 85 a 92 anteriores, la conservación de direcciones IP, basada en una medida legislativa con arreglo al artículo 15, apartado 1, de la Directiva 2002/58, a efectos del objetivo de luchar contra las infracciones penales en general, puede estar justificado cuando las disposiciones para dicha conservación introducidas por el marco legislativo en cuestión cumplan una serie de requisitos destinados a garantizar, en esencia, una separación realmente hermética de las diferentes categorías de datos conservados, de modo que la combinación de datos pertenecientes a diferentes categorías sea realmente descartado. Cuando tales acuerdos de conservación se imponen a los proveedores de servicios de comunicaciones electrónicas, la conservación general e indiscriminada de direcciones IP no constituye una injerencia grave en la privacidad de los titulares de dichas direcciones, ya que esos datos no permiten sacar conclusiones precisas sobre su vida privada.

104 Por lo tanto, a la luz de la jurisprudencia recordada en los apartados 95 a 97 supra, cuando se establece dicho marco legislativo, el acceso a las direcciones IP conservadas con el objetivo de luchar contra las infracciones penales en general puede estar justificado como se refiere al artículo 15, apartado 1, de la Directiva 2002/58, cuando dicho acceso se autoriza con el único fin de identificar a la persona sospechosa de estar implicada en tales delitos.

105 Además, permitir a una autoridad pública como Hadopi tener acceso a datos relativos a la identidad civil asociada a una dirección IP pública que le envían organizaciones titulares de derechos con el único fin de identificar al titular de esa dirección utilizada para actividades en línea susceptibles de infringir derechos de autor o derechos afines, con vistas a imponerle una de las medidas previstas en el procedimiento de respuesta gradual, es coherente con la jurisprudencia del Tribunal de Justicia relativa al «derecho de información» en el marco de un procedimiento por infracción de derechos un derecho de propiedad intelectual en el sentido del 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 dicha jurisprudencia, si bien destacó que la aplicación de las medidas previstas por la Directiva 2004/48 no puede afectar al RGPD ni a la Directiva 2002/58, el Tribunal de Justicia declaró que el artículo 8, apartado 3, de la Directiva 2004/48, leído conjuntamente con el artículo 15, apartado 1, de la Directiva 2002/58 y el artículo 7, letra f), de la Directiva 95/46, no impide que los Estados miembros impongan a los proveedores de servicios de comunicaciones electrónicas la obligación de revelar datos personales a particulares para permitirles interponer acciones civiles por infracciones de derechos de autor, pero tampoco exige a dichos Estados miembros que establezcan tal obligación (véase, en este sentido, la sentencia de 17 de junio de 2021, *MICM* , C-597/19, EU:C:2021:492 , apartados 124 y 125 y jurisprudencia citada).

107 Dicho esto, en segundo lugar, a efectos de la evaluación específica del alcance de la injerencia en la intimidad que supone el acceso de una autoridad pública a datos personales, el contexto particular en el que se produce ese acceso y, en particular, todos los los datos y la información comunicados a esa autoridad de conformidad con la legislación nacional aplicable, incluidos los datos e información preexistentes que revelan contenidos, no pueden ignorarse (véase, por analogía, TEDH, 24 de abril de 2018, *Benedik c. Eslovenia* , CE:ECHR: 2018:0424JUD006235714, § 109).

108 Así, en el caso de autos, es necesario tener en cuenta, a efectos de dicha apreciación, el hecho de que, antes de acceder a los datos relativos a la identidad civil de que dispone, Hadopi recibe de las organizaciones titulares de derechos, entre otras cosas, «información sobre las obras protegidas o la materia afectada por la conducta» y, «cuando proceda», el «nombre del archivo tal como aparece en el dispositivo del abonado», de conformidad con el punto 1 del anexo del Decreto n.º 2010- 236.

109 De los autos, sujetos a verificación por el órgano jurisdiccional remitente, se desprende que la información sobre la obra de que se trata –tal como consta en un informe cuyo contenido se rige por las deliberaciones de la CNIL de 10 de junio de 2010– es limitada, esencialmente , al título de la obra de que se trate y a un extracto denominado «fragmento», en forma de secuencia alfanumérica y no de captura de audio o vídeo de la obra.

110 A este respecto, es cierto que, en términos generales, no puede excluirse que el acceso por parte de una autoridad pública a un número limitado de datos relativos a la identidad civil del titular de una dirección IP notificada a dicha autoridad por un proveedor de servicios servicios de comunicaciones electrónicas con el único fin de identificar al titular de esa dirección cuando ésta haya sido utilizada para actividades susceptibles de infringir los derechos de autor o derechos afines, si se combina con un análisis de información, incluso limitada, sobre el contenido de la obra puesta a disposición ilegalmente en Internet que haya sido enviada previamente a esa autoridad por las organizaciones titulares de derechos, puede revelar a dicha autoridad pública ciertos aspectos de la vida privada de ese titular, incluida información sensible como la orientación sexual, opiniones políticas, creencias religiosas, filosóficas, sociales o de otro tipo y estado de salud. Además, dichos datos gozan de una protección especial según la legislación de la UE.

111 Sin embargo, en el presente caso, habida cuenta de la naturaleza limitada de los datos y de la información de que dispone Hadopi, sólo en situaciones atípicas pueden revelar información potencialmente sensible sobre aspectos de la vida privada del individuo en cuestión que , en conjunto, podrían permitir a esa autoridad pública extraer conclusiones precisas sobre su vida privada, por ejemplo estableciendo un perfil detallado de esa persona.

112 Ese podría ser el caso, inter alia, con respecto a una persona cuya dirección IP ha sido utilizada para actividades que infringen los derechos de autor o derechos conexos en redes peer-to-peer repetidamente, o en gran escala, en relación con obras protegidas de particular interés. tipos que pueden agruparse en función de las palabras de su título y que pueden revelar información potencialmente sensible sobre aspectos de su vida privada.

113 Dicho esto, varios factores respaldan la opinión de que, en el presente caso, la injerencia en la privacidad de una persona sospechosa de haber realizado una actividad que infringe los derechos de autor o derechos afines permitidos por una legislación como la controvertida en el litigio principal es no necesariamente de un alto grado de gravedad. En primer lugar, conforme a dicha legislación, el acceso de Hadopi a los datos personales en cuestión está restringido a un número limitado de funcionarios autorizados y jurados de esa autoridad pública, organismo que además tiene un estatuto independiente de conformidad con el artículo L. 331-12. del IPC. A continuación, el único objetivo de ese acceso es identificar a una persona sospechosa de haber participado en una actividad que infringe los derechos de autor o derechos afines cuando se descubre que una obra protegida ha sido puesta a disposición ilegalmente a través de la conexión a Internet de esa persona. Por último, el acceso de Hadopi a los datos personales en cuestión se limita estrictamente a los datos necesarios para tal fin (véase, por analogía, TEDH, 17 de octubre de 2019, *López Ribalda y otros c. España* , CE:ECHR:2019:1017JUD000187413, §§ 126 y 127).

114 Otro factor que puede reducir aún más el grado de injerencia en los derechos fundamentales a la protección de la intimidad y de los datos personales resultante de ese acceso por parte de Hadopi –que parece desprenderse de los autos que obran ante el Tribunal de Justicia, pero que corresponde comprobar al órgano jurisdiccional remitente– – se refiere al hecho de que, según la legislación nacional aplicable, los funcionarios de Hadopi que tienen acceso a los datos y a la información en cuestión están sujetos a una obligación de confidencialidad que les prohíbe revelar dichos datos e información en cualquier forma, excepto con el único fin de remitirlos el asunto al ministerio fiscal, y utilizarlos para fines distintos de la identificación del titular de la dirección IP sospechoso de haber

realizado una actividad que infringe los derechos de autor o un derecho afín para imponerle una de las medidas previstas en el contexto 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, en la medida en que la legislación nacional cumple los requisitos establecidos en el anterior apartado 101, las direcciones IP comunicadas a una autoridad pública como Hadopi no permiten rastrear el flujo de clics del titular de dichas direcciones, lo que tiende a confirmar la constatación de que la injerencia que supone el acceso de dicha autoridad a los datos de identificación controvertidos en el litigio principal no puede calificarse de grave.

116 En tercer lugar, debe recordarse que, para lograr el equilibrio necesario entre los derechos e intereses en conflicto impuesto por el requisito de proporcionalidad establecido en el artículo 15, apartado 1, primera frase, de la Directiva 2002/ 58, aunque la libertad de expresión y la confidencialidad de los datos personales son consideraciones primordiales y los usuarios de los servicios de telecomunicaciones e Internet deben tener una garantía de que se respetará su privacidad y su libertad de expresión, esos derechos fundamentales no son absolutos. Al equilibrar los derechos e intereses en cuestión, esos derechos fundamentales deben ceder en ocasiones ante otros derechos fundamentales o imperativos de interés público, como el mantenimiento del orden público y la prevención del delito o la protección de los derechos y libertades de los demás. Este es, en particular, el caso cuando la importancia otorgada a esas consideraciones primarias es tal que obstaculiza la eficacia de una investigación penal, en particular al hacer imposible o excesivamente difícil identificar efectivamente al autor de un delito penal e imponer una pena pena para él o ella (véase, por analogía, TEDH, 2 de marzo de 2009, *KU contra Finlandia* , CE:ECHR:2008:1202JUD000287202, § 49).

117 En este contexto, debe tenerse debidamente en cuenta que, como ya ha declarado el Tribunal de Justicia, en el caso de los delitos cometidos en línea, el acceso a las direcciones IP puede ser el único medio de investigación que permita a la persona a la que se asignó dicha dirección en el momento 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, UE :C:2020:791, apartado 154).

118 Esto tiende a demostrar, como también señaló, en esencia, el Abogado General en el punto 59 de sus conclusiones de 28 de septiembre de 2023, que la conservación y el acceso a dichas direcciones IP son, en lo que se refiere a la lucha contra infracciones penales como las infracciones de los derechos de autor, o derechos afines cometidos en línea – estrictamente necesarios para alcanzar el objetivo perseguido y, por tanto, cumplen el requisito de proporcionalidad impuesto por el artículo 15, apartado 1, de la Directiva 2002/58, leído a la luz del considerando 11 de dicha Directiva y del artículo 52, apartado 2.) de la Carta.

119 Además, como subrayó, en esencia, 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, no permitir dicho acceso conllevaría un riesgo real de daño sistémico. impunidad no sólo para los delitos que infringen los derechos de autor o derechos conexos, sino también para otros tipos de delitos cometidos en línea o cuya comisión o preparación se ve facilitada por las características específicas de Internet. La existencia de tal riesgo constituye un factor pertinente a efectos de evaluar, al sopesar los distintos derechos e intereses en cuestión, si una injerencia en los derechos garantizados por los artículos 7, 8 y 11 de la Carta es una medida proporcionada a la luz de del objetivo de luchar contra las infracciones penales.

120 Es cierto que el acceso por parte de una autoridad pública como Hadopi a datos de identidad civil asociados con la dirección IP desde la que se cometió el delito en línea no es necesariamente el

único medio posible de investigación para identificar a la persona que poseía esa dirección en ese momento. se cometió ese delito. Esta identificación también podría ser posible, a primera vista, examinando todas las actividades en línea de la persona en cuestión, en particular analizando las "huellas" que esa persona podría haber dejado en las redes sociales, como el nombre de usuario utilizado en dichas redes. 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 medio de investigación sería especialmente intrusivo, ya que podría revelar información precisa sobre la vida privada de los interesados. Por tanto, supondría para dichas personas una injerencia más grave en los derechos garantizados por los artículos 7, 8 y 11 de la Carta que la que se derivaría de una normativa como la controvertida en el litigio principal.

122 De lo anterior se desprende que el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta debe interpretarse en el sentido de que no se opone, en En principio, la legislación nacional permite a una autoridad pública responsable de la protección de los derechos de autor y derechos afines contra las infracciones de esos derechos cometidas en Internet acceder a datos relacionados con la identidad civil asociados con direcciones IP previamente recopiladas por organizaciones titulares de derechos y conservadas por los proveedores de servicios electrónicos. servicios de comunicaciones de forma separada y verdaderamente hermética, con el único fin de permitir a dicha autoridad identificar a los titulares de las direcciones sospechosas de ser responsables de dichas infracciones y, en su caso, adoptar medidas al respecto. En ese caso, la legislación nacional debe prohibir a los funcionarios que tengan dicho acceso (i) revelar, bajo cualquier forma, información relativa al contenido de los expedientes consultados por dichos titulares, salvo con el único fin de remitir el asunto al Ministerio Fiscal, (ii) rastrear de cualquier forma el flujo de clics de dichos titulares y (iii) utilizar esas direcciones IP para fines distintos a la adopción de dichas medidas.

El requisito de una revisión previa por parte de un tribunal o de un organismo administrativo independiente antes de que una autoridad pública acceda a datos relacionados con la identidad civil asociada a una dirección IP.

123 Sin embargo, se plantea la cuestión de si el acceso de la autoridad pública a los datos relativos a la identidad civil asociada a una dirección IP también debe estar sujeto a un control previo por parte de un tribunal o de un organismo administrativo independiente.

124 A este respecto, el Tribunal de Justicia ha declarado que es para garantizar, en la práctica, el pleno respeto de las condiciones que los Estados miembros deben establecer para garantizar que el acceso se limita a lo estrictamente necesario. "esencial" que el acceso de las autoridades nacionales competentes a los datos de tráfico y de localización esté sujeto a un control previo llevado a cabo por un tribunal o por un organismo administrativo 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 exige, en primer lugar, que el tribunal o el órgano administrativo independiente encargado de ejercerlo tenga todas las competencias y ofrezca todas las garantías necesarias para conciliar los distintos intereses y derechos legítimos en conflicto. En particular, en el caso de una investigación penal, dicho control exige que dicho órgano jurisdiccional o organismo pueda lograr un justo equilibrio entre, por un lado, los intereses legítimos relacionados con las necesidades de la

investigación en el contexto de 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 de las personas cuyos datos son objeto del acceso (sentencia de 5 de abril de 2022, *Comisario de An Garda Síochána y otros* , C- 140/20, EU:C:2022:258, apartado 107 y jurisprudencia citada).

126 En segundo lugar, cuando ese control no lo lleva a cabo un tribunal sino un organismo administrativo independiente, dicho organismo debe tener un estatuto que le permita actuar de forma objetiva e imparcial en el ejercicio de sus funciones y, a tal efecto, debe estar libre de cualquier responsabilidad. influencia externa. De ello se deduce que el requisito de independencia que debe cumplir el organismo encargado de realizar el control previo implica que dicho organismo debe ser un tercero respecto de la autoridad que solicita el acceso a los datos, para que el primero es capaz de llevar a cabo la revisión de manera objetiva e imparcial y libre de cualquier influencia externa. En particular, en el ámbito penal la exigencia de independencia implica que el órgano encargado del control previo, por un lado, no debe participar en el desarrollo de la investigación penal en cuestión y, por otro, debe mantener una postura neutral frente a las partes en el proceso 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 lugar, el control independiente exigido con arreglo al artículo 15, apartado 1, de la Directiva 2002/58 debe tener lugar antes de cualquier acceso a los datos de que se trate, salvo en caso de urgencia debidamente justificada, en cuyo caso el control debe tener lugar en un plazo poco tiempo. Un control posterior no permitiría alcanzar el objetivo de un control previo, consistente en impedir la autorización de un acceso a los datos en cuestión que exceda de lo estrictamente necesario (sentencia de 5 de abril de 2022, *Comisario de An Garda Síochána y otros* , C-140/20, EU:C:2022:258, apartado 110).

128 Dicho esto, aunque, como se desprende de la jurisprudencia mencionada en el apartado 124 supra, el Tribunal de Justicia ha sostenido que es "esencial" que el acceso de las autoridades nacionales competentes a los datos de tráfico y de localización esté sujeto a un control previo llevada a cabo por un tribunal o por un organismo administrativo independiente, dicha jurisprudencia se desarrolló en el contexto de medidas nacionales que permiten, a efectos de un objetivo vinculado a la lucha contra la delincuencia grave, el acceso general a todos los datos de tráfico y de localización conservados, independientemente de si existía algún vínculo con el objetivo perseguido y que, por tanto, implicaba injerencias graves e incluso "particularmente graves" en los derechos fundamentales de que se trata.

129 Por el contrario, en los asuntos que se referían a las condiciones en las que el acceso a datos relativos a la identidad civil podría estar justificado con arreglo al artículo 15, apartado 1, de la Directiva 2002/58, leído a la luz de los artículos 7, 8 y 11 de la Carta, no El Tribunal de Justicia hizo referencia expresa a la exigencia de dicho 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; , *Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas)* , C-746/18, EU:C:2021:152, apartado 34).

130 De la jurisprudencia del Tribunal de Justicia relativa al principio de proporcionalidad, cuyo cumplimiento exige la primera frase del apartado 1 del artículo 15 de la Directiva 2002/58 (en particular, la jurisprudencia según la cual la cuestión de si la Los Estados miembros pueden justificar una limitación de los derechos y obligaciones establecidos, entre otros, en los artículos 5, 6 y 9 de dicha Directiva, debe evaluarse midiendo la gravedad de la injerencia en los derechos fundamentales establecidos en los artículos 7, 8 y 11. de la Carta que implica tal limitación y verificando que la importancia del objetivo de interés público perseguido por esa limitación es

proporcionada a esa 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) – que el grado de injerencia en los derechos fundamentales implicados por el acceso a los datos personales en cuestión y el grado de sensibilidad de dichos datos deben también influyen en las salvaguardias sustantivas y procesales a las que debe estar sujeto ese acceso, incluido el requisito de una revisión previa por parte de un tribunal o de un órgano administrativo independiente.

131 Por lo tanto, teniendo en cuenta este principio de proporcionalidad, procede declarar que la exigencia de un control previo por parte de un tribunal o de un organismo administrativo independiente es necesaria cuando, en el contexto de una legislación nacional que permite a una autoridad pública acceder a datos personales, dicho acceso entraña el riesgo de una grave injerencia en los derechos fundamentales de la persona de que se trate, en la medida en que podría permitir a dicha autoridad pública extraer conclusiones precisas sobre la vida privada de dicha persona y, en su caso, establecer un perfil detallado de su persona. esa persona.

132 Por el contrario, esta exigencia de control previo no se aplica cuando la injerencia en los derechos fundamentales de que se trata que implica el acceso de una autoridad pública a datos personales no puede calificarse de grave.

133 Así ocurre con el acceso a datos relativos a la identidad civil de los usuarios de comunicaciones electrónicas con el único fin de identificar al usuario de que se trate, y sin que dichos datos puedan asociarse a información sobre las comunicaciones realizadas, ya que, según Según la jurisprudencia del Tribunal de Justicia, las intromisiones que supone dicho tratamiento de dichos datos no pueden, en principio, calificarse de graves (véase, en este sentido, la sentencia de 6 de octubre de 2020, *La Quadrature du Net y otros* , C-511 /18, C-512/18 y C-520/18, EU:C:2020:791, apartados 157 y 158).

134 De ello se deduce que, cuando se establece un marco de conservación como el descrito en los apartados 86 a 89 supra, el acceso de la autoridad pública a los datos relativos a la identidad civil asociados a las direcciones IP así conservadas no está, en principio, sujeto a el requisito de revisión previa por un tribunal o por un órgano administrativo independiente.

135 Dicho esto, como se señaló en los apartados 110 y 111 supra, no se puede descartar que, en situaciones atípicas, los datos y la información limitados puestos a disposición de una autoridad pública en el contexto de un procedimiento como el procedimiento de respuesta gradual en cuestión en el litigio principal puede revelar información potencialmente sensible sobre aspectos de la vida privada del interesado que, en conjunto, podrían permitir a dicha autoridad pública extraer conclusiones precisas sobre la vida privada de dicha persona y, en su caso, establecer un perfil detallado de esa persona.

136 Como se señaló en el párrafo 112 supra, ese riesgo para la privacidad puede surgir, entre otras cosas, cuando una persona participa en actividades que infringen los derechos de autor o derechos conexos en redes entre pares de manera repetida o a gran escala, en relación con obras protegidas. de tipos particulares que pueden agruparse en función de las palabras de su título, revelando información potencialmente sensible sobre aspectos de la vida privada de esa persona.

137 Así, en el presente caso, en el contexto del procedimiento administrativo de respuesta gradual, el titular de una dirección IP puede estar especialmente expuesto a tal riesgo para su privacidad cuando ese procedimiento llega a la fase en la que Hadopi debe decidir si no recurrir al Ministerio Fiscal para que se procese a dicha persona por conductas que puedan constituir un delito leve de negligencia grave o un delito de falsificación.

138 Esta remisión presupone que el titular de una dirección IP ya haya recibido dos recomendaciones y una carta de notificación en la que se le informe de que sus actividades pueden ser objeto de persecución penal, medidas que implican que, en cada ocasión, Hadopi haya tenido acceso a datos relativos a la identidad civil de aquella persona cuya dirección IP ha sido utilizada para actividades que infringen los derechos de autor o derechos afines y a un fichero relativo a la obra en cuestión que contiene, esencialmente, su título.

139 No se puede excluir que, en su conjunto y a medida que se desarrolla el procedimiento administrativo de respuesta escalonada, los datos así facilitados en las distintas fases de dicho procedimiento puedan revelar informaciones concordantes y potencialmente sensibles sobre aspectos de la vida privada del interesado, por lo que posible establecer un perfil de esa persona.

140 Por lo tanto, es probable que la intensidad de la infracción del derecho al respeto de la vida privada aumente a medida que el procedimiento de respuesta gradual, que es un proceso secuencial, avanza a través de sus diversas etapas.

141 En el caso de autos, el acceso de Hadopi a todos los datos relativos al interesado recopilados durante las distintas fases de dicho procedimiento puede permitir, mediante la vinculación de dichos datos, extraer conclusiones precisas sobre la vida privada de dicho interesado. persona. Por lo tanto, en el marco de un procedimiento como el procedimiento de respuesta gradual controvertido en el litigio principal, la legislación nacional también debe prever un control previo por parte de un tribunal o de un organismo administrativo independiente, que cumpla las condiciones establecidas en los apartados 125 a 127. supra, en una determinada fase de dicho procedimiento, a fin de descartar riesgos de injerencias desproporcionadas en los derechos fundamentales a la protección de la intimidad y de los datos personales del interesado. Esto significa que, en la práctica, dicha revisión debe tener lugar antes de que Hadopi pueda vincular los datos de identidad civil de una persona asociados a una dirección IP y obtenidos de un proveedor de servicios de comunicaciones electrónicas (esa persona ya ha sido objeto de dos recomendaciones). y el archivo relativo a la obra puesto a disposición en Internet para que otros lo descarguen. Por lo tanto, ese control debe tener lugar antes de enviar una carta de notificación, tal como se contempla en el artículo R. 331-40 del CPI, declarando que dicha persona ha incurrido en una conducta que puede constituir un delito leve de negligencia grave. Sólo después de dicha revisión previa por parte de un tribunal o de una autoridad administrativa independiente y de la autorización de dicho tribunal o autoridad administrativa, Hadopi podrá enviar dicha carta y luego, si es necesario, remitir el asunto al ministerio fiscal con con vistas a la persecución de ese delito.

142 Debe permitirse a Hadopi identificar los casos en los que el titular de la dirección IP en cuestión alcanza esa tercera etapa de dicho procedimiento de respuesta gradual. En consecuencia, dicho procedimiento debe organizarse y estructurarse de manera que los datos de identidad civil de una persona asociados a direcciones IP previamente recopiladas en Internet, obtenidas de proveedores de servicios de comunicaciones electrónicas, no puedan ser vinculados automáticamente por los responsables de la examen de los hechos en Hadopi, cuyos ficheros contienen información que revela los títulos de las obras protegidas cuya puesta a disposición en Internet justificaba esa recogida de direcciones IP.

143 Así, esa vinculación a efectos de la tercera etapa del procedimiento gradual debe suspenderse cuando la obtención de esos datos de identidad civil, correspondientes a un caso en el que posiblemente se haya repetido por segunda vez una actividad violatoria de los derechos de autor o de derechos afines, desencadena el requisito de una revisión previa por parte de un tribunal o de un organismo administrativo independiente descrito en el párrafo 141 supra.

144 Además, la organización del requisito de control previo a que se refieren los apartados 141 a 143 anteriores, al limitarse a la tercera etapa del procedimiento de respuesta gradual y no aplicarse a las etapas anteriores de dicho procedimiento, también permite tener en cuenta Cabe partir del argumento de que es necesario garantizar la viabilidad de ese procedimiento, que se caracteriza – especialmente en las etapas previas al posible envío de la carta de notificación y, en su caso, a la remisión del asunto al público fiscalía – por el enorme número de solicitudes de acceso por parte de la autoridad pública resultantes del igualmente elevado número de informes remitidos por las organizaciones de titulares de derechos.

145 Además, por lo que respecta al objeto del control previo mencionado en los apartados 141 a 143 supra, de la jurisprudencia recordada en los apartados 95 y 96 supra se desprende que, cuando el interesado sea sospechoso de haber cometido el delito de « negligencia grave», definida en el artículo R. 335-5 del IPC, que está comprendida en el ámbito de las infracciones penales en general, el tribunal o el organismo administrativo independiente responsable de dicho control deberá denegar el acceso cuando dicho acceso lo permitiría a la autoridad pública que lo solicitó sacar conclusiones precisas sobre la vida privada de esa persona.

146 Sin embargo, incluso el acceso que permita sacar conclusiones tan precisas debe autorizarse en los casos en que las pruebas presentadas ante dicho tribunal o organismo administrativo independiente apoyen la sospecha de que la persona ha cometido el delito de falsificación contemplado en el artículo L. 335-2 del CPI o el artículo L. 335-4 de dicho Código, dado que un Estado miembro puede considerar que tal infracción, en la medida en que menoscabe un interés fundamental de la sociedad, constituye un delito grave.

147 Por último, en cuanto a la forma en que debe llevarse a cabo ese control previo, el Gobierno francés alega que, habida cuenta de las características particulares del acceso de Hadopi a los datos en cuestión, en particular de su magnitud masiva, sería adecuado que una revisión previa, si fuera requerida, que será totalmente automatizada. Según dicho Gobierno, dicho control, de carácter puramente objetivo, tiene por objeto esencialmente comprobar que el informe remitido a Hadopi contiene todas las informaciones y datos requeridos, sin que Hadopi esté obligada a realizar ninguna evaluación de dichas informaciones o datos. .

148 Sin embargo, un control previo en ningún caso puede ser enteramente automatizado ya que, como se desprende de la jurisprudencia recordada en el apartado 125 supra, en el caso de una investigación penal, dicho control es un requisito, en cualquier caso , que el tribunal o el organismo administrativo independiente en cuestión debe poder lograr un justo equilibrio entre, por un lado, los intereses legítimos relacionados con las necesidades de la investigación en el contexto de la lucha contra la delincuencia y, por otro, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de las personas cuyos datos son objeto del acceso.

149 Esta ponderación de los distintos intereses y derechos legítimos en cuestión requiere la intervención de una persona física, tanto más cuanto que el carácter automático y la gran escala del tratamiento de datos en cuestión plantean riesgos para la privacidad.

150 Además, un control enteramente automatizado no es, por regla general, capaz de garantizar que el acceso no vaya más allá de los límites de lo estrictamente necesario y que las personas cuyos datos personales estén en juego tengan salvaguardias efectivas contra los riesgos de abuso y contra cualquier acceso o uso ilegal de dichos datos.

151 Así, si bien las revisiones automatizadas pueden permitir verificar parte de la información contenida en los informes de las organizaciones titulares de derechos, dichas revisiones deben, en cualquier

caso, ir de la mano de revisiones realizadas por personas físicas que cumplan plenamente los requisitos establecidos en los párrafos 125 a 127 arriba.

Los requisitos relativos a las condiciones sustantivas y procesales y a las salvaguardias contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos de dichos datos aplicables al acceso por parte de una autoridad pública a datos relativos a la identidad civil asociada a una dirección IP

152 De la jurisprudencia del Tribunal de Justicia se desprende que el acceso a datos personales sólo puede satisfacer el requisito de proporcionalidad impuesto por el artículo 15, apartado 1, de la Directiva 2002/58 si el acto legislativo que lo autoriza establece, mediante disposiciones claras y precisas normas, que ese acceso esté sujeto al cumplimiento de las condiciones materiales y procesales aplicables y que los interesados dispongan de garantías efectivas contra los riesgos de acceso o utilización abusiva o ilícita 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 datos relativos a las comunicaciones electrónicas)* , C-746/18, EU:C:2021:152, apartado 49 y jurisprudencia citada).

153 Como ha señalado el Tribunal de Justicia, la necesidad de tales garantías es aún mayor cuando los datos personales son objeto de 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 formulada por el Tribunal de Justicia con vistas a la vista del 5 de julio de 2022, el Gobierno francés confirmó que, como establece, por otra parte, el artículo L. 331-29 del CPI, el acceso de Hadopi a Los datos relativos a la identidad civil en el marco del procedimiento de respuesta escalonada son el resultado de un tratamiento de datos esencialmente automatizado, lo que se explica por el enorme número de casos de falsificación detectados en redes peer-to-peer por organizaciones titulares de derechos, que son notificados a Hadopi en la forma de los informes.

155 De los autos se desprende, en particular, que, durante ese tratamiento de datos, los funcionarios de Hadopi comprueban –de forma esencialmente automatizada y sin evaluar los hechos de que se trata como tales– si los informes remitidos a dicha autoridad contienen todos los datos la información y los datos enumerados en el punto 1 del anexo del Decreto n.o 2010-236, en particular las circunstancias de hecho relacionadas con la puesta a disposición ilegal en Internet de que se trate y las direcciones IP utilizadas a tal efecto. Dicho procesamiento debe ir acompañado de revisiones por parte de personas físicas.

156 Dado que es probable que dicho procesamiento automatizado implique un cierto número de falsos positivos y, sobre todo, el riesgo de que terceros utilicen indebidamente una cantidad potencialmente muy significativa de datos personales con fines ilegales o abusivos, es importante que, en virtud de un medida legislativa, el sistema de tratamiento de datos utilizado por una autoridad pública es objeto, a intervalos regulares, de un control por parte de un organismo independiente que actúa como tercero frente a dicha autoridad, destinado a verificar la integridad del sistema, incluida la eficacia las salvaguardias contra los riesgos de abuso y contra todo acceso o utilización ilícita de dichos datos que dicho sistema debe garantizar, así como la eficacia y fiabilidad de dicho sistema para detectar conductas infractoras que puedan calificarse, en caso de repetición, de negligencia grave o falsificación.

157 Por último, procede añadir que el tratamiento de datos personales por parte de una autoridad pública, como el realizado por Hadopi en el marco del procedimiento de respuesta gradual, debe respetar las normas específicas para la protección de dichos datos establecidas por Directiva 2016/680, cuya finalidad, según su artículo 1, es establecer las normas relativas a la protección de

las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes con fines de prevención, investigación, detección o el enjuiciamiento de delitos penales o la ejecución de sanciones penales, incluida la protección y prevención de amenazas a la seguridad pública.

158 En el presente caso, incluso si, según la legislación nacional aplicable, no tiene poderes de decisión propios, Hadopi, cuando procesa datos personales en el contexto del procedimiento de respuesta gradual y adopta medidas tales como una recomendación o una notificación al interesado de que la conducta en cuestión es objeto de persecución penal debe ser clasificada como «autoridad pública», en el sentido del artículo 3 de la Directiva 2016/680, implicada en la prevención, investigación, detección o enjuiciamiento de delitos penales, a saber, el delito leve de negligencia grave o el delito de falsificación, y, por tanto, entra en el ámbito de aplicación de dicha Directiva, de conformidad con su artículo 1.

159 A este respecto, el Gobierno francés afirmó, en respuesta a una pregunta que le planteó el Tribunal de Justicia con vistas a la vista del 5 de julio de 2022, que, dado que las medidas adoptadas por Hadopi en el marco del procedimiento de respuesta gradual «son de «de carácter precriminal directamente vinculado al proceso judicial», el sistema de gestión de medidas de protección de obras en Internet, aplicado por Hadopi, está sujeto, como se desprende de la jurisprudencia del tribunal remitente, a las disposiciones del Derecho nacional destinadas a transponer la Directiva 2016/680.

160 Por el contrario, dicho procesamiento de datos por parte de Hadopi no entra dentro del alcance del RGPD. El artículo 2, apartado 2, letra d), del RGPD establece que dicho Reglamento 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 la ejecución de sanciones penales, incluidas la salvaguardia y prevención de amenazas a la seguridad pública.

161 Como señaló el Abogado General en el punto 104 de sus conclusiones de 27 de octubre de 2022, dado que Hadopi debe cumplir la Directiva 2016/680 en el marco del procedimiento de respuesta gradual, las personas implicadas en dicho procedimiento deben disfrutar de un conjunto de derechos sustantivos. y garantías procesales, incluido el derecho de acceso, rectificación y eliminación de datos personales procesados por Hadopi y la posibilidad de presentar una queja ante una autoridad supervisora independiente, seguida, cuando corresponda, de un recurso judicial en las condiciones de la ley general.

162 En este contexto, de la normativa nacional controvertida en el litigio principal se desprende que, en el marco del procedimiento de respuesta gradual, más concretamente en el momento de envío de la segunda recomendación y en el momento de la notificación posterior, la conducta puede constituir un delito penal, el destinatario de esas comunicaciones disfruta de determinadas garantías procesales, como el derecho a presentar observaciones, el derecho a obtener información sobre la conducta delictiva que presuntamente ha cometido y, en lo que respecta a esa notificación , el derecho a solicitar una audiencia y a ser asistido por un abogado.

163 En cualquier caso, corresponde al tribunal remitente comprobar si dicha legislación nacional establece todas las garantías materiales y procesales previstas por la Directiva 2016/680.

164 Habida cuenta de todas las consideraciones anteriores, procede responder a las tres cuestiones prejudiciales que el artículo 15, apartado 1, de la Directiva 2002/58, leído a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1,) de la Carta, debe interpretarse en el sentido de que no se opone a una legislación nacional que autoriza a la autoridad pública responsable de la protección de los derechos de autor y derechos afines contra las infracciones de dichos derechos cometidas en

Internet a acceder a los datos conservados por los proveedores de servicios de comunicaciones electrónicas disponibles al público, en relación con la identidad civil asociada a las direcciones IP previamente recopiladas por organizaciones titulares de derechos, de modo que dicha autoridad pueda identificar a los titulares de dichas direcciones –que han sido utilizadas para actividades que pueden constituir tales infracciones– y pueda, en su caso, tomar medidas contra ellos, siempre que, conforme a esa legislación:

– dichos datos se conservan en condiciones y de conformidad con disposiciones técnicas que garantizan que no existe la posibilidad de que dicha conservación permita extraer conclusiones precisas sobre la vida privada de los titulares de dichas direcciones IP, por ejemplo estableciendo un perfil detallado de dichas personas. excluido, lo que puede lograrse, en particular, imponiendo a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar las distintas categorías de datos personales, como los datos relativos a la identidad civil, las direcciones IP y los datos de tráfico y de localización, de tal manera para garantizar una separación verdaderamente hermética de esas diferentes categorías de datos, impidiendo así, en la fase de conservación, cualquier uso combinado de esas diferentes categorías de datos (y durante un período que no exceda lo estrictamente necesario);

– que el acceso de la autoridad pública a dichos datos conservados por separado y de forma realmente hermética sirva exclusivamente para identificar a la persona sospechosa de haber cometido un delito y esté sujeto a las garantías necesarias para garantizar que dicho acceso no pueda, salvo en situaciones atípicas, permitir datos precisos conclusiones que deben extraerse sobre la vida privada de los titulares de direcciones IP, por ejemplo estableciendo un perfil detallado de dichas personas, lo que implica, en particular, que los funcionarios de dicha autoridad autorizados a tener dicho acceso tienen prohibido revelar, en cualquier forma en ningún caso, información sobre el contenido de los ficheros consultados por dichos titulares, salvo con el único fin de remitir el asunto al Ministerio Fiscal, del seguimiento del flujo de clics de dichos titulares de direcciones IP y, más en general, de la utilización de dichas direcciones IP para cualquier finalidad distinta de la de identificar a sus titulares con vistas a la posible adopción de medidas contra ellos;

– se excluye la posibilidad, para los responsables del examen de los hechos en el seno de dicha autoridad pública, de vincular dichos datos a ficheros que contengan informaciones que revelen el título de las obras protegidas cuya puesta a disposición en Internet justificó la recogida de direcciones IP por parte de las organizaciones de titulares de derechos sujeto, en los casos en que la misma persona repite nuevamente una actividad que infringe los derechos de autor o derechos conexos, a una revisión por parte de un tribunal o de un organismo administrativo independiente, que no puede automatizarse completamente y debe tener lugar antes de cualquier enlace, en la medida en que dicho enlace sea capaz, en tales circunstancias, de permitir extraer conclusiones precisas sobre la vida privada de la persona cuya dirección IP ha sido utilizada para actividades que pueden infringir los derechos de autor o derechos afines;

– el sistema de procesamiento de datos utilizado por la autoridad pública esté sujeto a intervalos regulares a una revisión, por parte de un organismo independiente que actúa como tercero en relación con dicha autoridad pública, destinada a verificar la integridad del sistema, incluidas las salvaguardias efectivas contra la riesgos de acceso abusivo o ilegal o uso de esos datos, y su efectividad y confiabilidad para detectar posibles conductas infractoras.

Costos

165 Dado que el presente procedimiento constituye, para las partes del litigio principal, un incidente pendiente ante el órgano jurisdiccional remitente, corresponde a éste resolver sobre las costas. Los gastos incurridos al presentar observaciones ante el Tribunal, distintos de los de dichas partes, no son recuperables.

Por todo lo expuesto, el Tribunal (Pleno) resuelve:

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 datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y comunicaciones electrónicas), así como modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, leída a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea,

debe interpretarse en el sentido de que no se opone a la legislación nacional que autoriza a la autoridad pública responsable de la protección de los derechos de autor y derechos afines contra las infracciones de dichos derechos cometidas en Internet a acceder a los datos, conservados por los proveedores de servicios de comunicaciones electrónicas disponibles al público, relacionados con la identidad civil. asociadas a direcciones IP previamente recopiladas por organizaciones titulares de derechos, de modo que dicha autoridad pueda identificar a los titulares de dichas direcciones –que han sido utilizadas para actividades que puedan constituir tales infracciones– y pueda, en su caso, tomar medidas contra ellos, siempre que, en virtud de dicha legislación:

– **dichos datos se conservan en condiciones y de conformidad con disposiciones técnicas que garantizan que no existe la posibilidad de que dicha conservación permita extraer conclusiones precisas sobre la vida privada de los titulares de dichas direcciones IP, por ejemplo estableciendo un perfil detallado de dichas personas. excluido, lo que puede lograrse, en particular, imponiendo a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar las distintas categorías de datos personales, como los datos relativos a la identidad civil, las direcciones IP y los datos de tráfico y de localización, de tal manera para garantizar una separación verdaderamente hermética de esas diferentes categorías de datos, impidiendo así, en la fase de conservación, cualquier uso combinado de esas diferentes categorías de datos (y durante un período que no exceda lo estrictamente necesario);**

– **que el acceso de la autoridad pública a dichos datos conservados separadamente y de forma verdaderamente hermética sirva exclusivamente para identificar a la persona sospechosa de haber cometido un delito y esté sujeto a las garantías necesarias para garantizar que dicho acceso no pueda, salvo en situaciones atípicas, permitir datos precisos conclusiones que deben extraerse sobre la vida privada de los titulares de direcciones IP, por ejemplo estableciendo un perfil detallado de dichas personas, lo que implica, en particular, que los funcionarios de dicha autoridad autorizados a tener dicho acceso tienen prohibido revelar, en cualquier forma en ningún caso, información sobre el contenido de los ficheros consultados por dichos titulares, salvo con el único fin de remitir el asunto al Ministerio Fiscal, del seguimiento del flujo de clics de dichos titulares de direcciones IP y, más en general, de la utilización de dichas direcciones IP para cualquier finalidad distinta de la de identificar a sus titulares con vistas a la posible adopción de medidas contra ellos;**

– **se excluye la posibilidad, para los responsables del examen de los hechos en el seno de dicha autoridad pública, de vincular dichos datos a ficheros que contengan informaciones que revelen el título de las obras protegidas cuya puesta a disposición en Internet justificó la recogida de direcciones IP por parte de las organizaciones de titulares de derechos sujeto, en los casos en que la misma persona repite nuevamente una actividad que infringe los derechos de autor o derechos conexos, a una revisión por parte de un tribunal o de un organismo administrativo independiente, que no puede automatizarse completamente y debe tener lugar antes de cualquier enlace, en la medida en que dicho enlace sea capaz, en tales circunstancias, de permitir extraer conclusiones precisas sobre la vida privada de la persona cuya dirección IP ha sido utilizada para actividades que pueden infringir los derechos de autor o derechos afines;**

– **el sistema de procesamiento de datos utilizado por la autoridad pública esté sujeto a intervalos regulares a una revisión, por parte de un organismo independiente que actúa como tercero en relación con dicha autoridad pública, destinada a verificar la integridad del sistema, incluidas las salvaguardias efectivas contra la riesgos de acceso abusivo o ilegal o uso de esos datos, y su efectividad y confiabilidad para detectar posibles conductas infractoras.**

[Firmas]