Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
SR. MACIEJ SZPUNAR
presentadas el 27 de octubre de 2022 [1]

Asunto C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
contra
Premier ministre,
Ministère de la Culture

[Petición de decisión prejudicial planteada por el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia)]

«Procedimiento prejudicial — Tratamiento de datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Artículo 15, apartado 1 — Facultad de los Estados miembros de limitar el alcance de determinados derechos y obligaciones — Obligación de control previo por un órgano jurisdiccional o una entidad administrativa independiente con poder vinculante — Datos de identidad civil correspondientes a una dirección IP»

I. Introducción

1. La cuestión de la conservación de determinados datos de los usuarios de Internet y el acceso a estos es una cuestión permanentemente de actualidad y es objeto de una jurisprudencia reciente pero ya abundante del Tribunal de Justicia.

2. El presente asunto brinda al Tribunal de Justicia la ocasión de examinar esta cuestión una vez más, en el contexto renovado de la lucha contra las violaciones de los derechos de propiedad intelectual cometidas exclusivamente en línea.

[1] Lengua original: francés.

II. Marco jurídico

A. Derecho de la Unión

3. Los considerandos 2, 6, 7, 11, 22, 26 y 30 de la Directiva 2002/58/CE [2] tienen el siguiente tenor:

«(2) La presente Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea [(en lo sucesivo, «Carta»)]. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de dicha Carta.

[…]

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

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

[…]

(11) Al igual que la Directiva 95/46/CE[[3]], la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales [, hecho en Roma el 4 de noviembre de 1950], según la interpretación que se hace de este en las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

[2] Directiva del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 2002, L 201, p. 37).

[3] Directiva 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).

[…]

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

[…]

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

[…]

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

4. A tenor de lo dispuesto en el artículo 2 de dicha Directiva, titulado «Definiciones»:

«[…]

Además, a efectos de la presente Directiva se entenderá por:

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

b) “datos de tráfico”: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;

c) “datos de localización”: cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;

d) “comunicación”: cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información;

[…]».

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

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

6. El artículo 5 de dicha Directiva, titulado «Confidencialidad de las comunicaciones», establece:

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

[…]

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

7. Con arreglo al artículo 6 de la Directiva 2002/58, titulado «Datos de tráfico»:

«1. Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.

2. Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

[…]»

8. El artículo 15, apartado 1, de dicha Directiva 2002/58, titulado «Aplicación de determinadas disposiciones de la Directiva [95/46]», establece lo siguiente:

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

B. Derecho francés

1. Código de la Propiedad Intelectual

9. El artículo L. 331-12 del code de la propriété intellectuelle (Código de la Propiedad Intelectual), en su versión aplicable al litigio principal (en lo sucesivo, «CPI»), prevé:

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

10. El artículo L. 331-13 del CPI está redactado en los siguientes términos:

«La [Hadopi] ejerce:

[…]

2.° la misión de proteger [las obras y objetos a los que estén ligados derechos de autor o derechos afines en las redes de comunicaciones electrónicas] contra las infracciones de esos derechos cometidas en las redes de comunicaciones electrónicas utilizadas para la prestación de servicios de comunicación al público en línea; […]».

11. De conformidad con el artículo L. 331-15 de dicho Código:

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

[…]

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

12. El artículo L. 331-17 del citado Código prevé:

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

13. A tenor de lo dispuesto en el artículo L. 331-21 de dicho Código:

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

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

Para las necesidades del procedimiento, podrán obtener todos los documentos, cualquiera que sea su soporte, incluidos los datos conservados y procesados por los operadores de comunicaciones electrónicas en virtud del artículo L. 34-1 del code des postes et des communications électroniques [(Código de Correos y Comunicaciones Electrónicas)] y los proveedores de servicios mencionados en los números 1 y 2 del apartado I del artículo 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(Ley n.º 2004-575, de 21 de junio de 2004, relativa a la Confianza en la Economía Digital)].

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

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

14. De conformidad con el artículo L. 331-24 del CPI:

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

– los organismos de defensa profesional debidamente constituidos;

– las entidades de gestión colectiva, y

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

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

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

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

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

En caso de que se repitan hechos que puedan constituir un incumplimiento de la obligación prevista en el artículo L. 336-3 en un plazo de seis meses a partir del envío de la recomendación a que se refiere el párrafo primero, la Comisión podrá remitir por vía electrónica una nueva recomendación que contenga la misma información que la anterior […]. Deberá acompañar dicha recomendación de una carta enviada con acuse de recibo o cualquier otro medio que sirva para establecer la prueba de la fecha de presentación de esta recomendación.

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

16. El artículo L. 331-29 del citado Código está redactado en los siguientes términos:

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

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

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

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

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

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

17. El artículo R. 331-37 de dicho Código prevé:

«Los operadores de comunicaciones electrónicas […] y los proveedores […] están obligados a comunicar, mediante la interconexión con el tratamiento automatizado de datos personales mencionado en el artículo L. 331-29 o recurriendo a un soporte de grabación que garantice su integridad y seguridad, los datos personales y la información mencionada en el punto 2.° del anexo del [décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du [CPI] dénommé " Système de gestion des mesures pour la protection des œuvres sur internet " (Decreto n.º 2010-236, de 5 de marzo de 2010, relativo al tratamiento automatizado de datos personales autorizado por el artículo L. 331-29 del [CPI] denominado "Sistema de gestión de medidas para la protección de las obras en Internet")[4]], en un plazo de ocho días contados a partir de la transmisión por la Comisión de Protección de los Derechos de los datos técnicos necesarios para la identificación del abonado cuyo acceso a datos de comunicación al público en línea se haya utilizado para la reproducción, representación, puesta a disposición o comunicación al público de obras u objetos protegidos sin autorización de los titulares de los derechos […], cuando se requiera tal autorización.

[…]»

18. El artículo R. 335-5 del CPI prevé:

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

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

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

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

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

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

4 JORF de 7 de marzo de 2010, texto n.º 19.

19. El artículo L. 336-3 de dicho Código dispone:

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

El incumplimiento de la obligación a que se refiere el párrafo primero por parte del titular del acceso no tiene por efecto exigir responsabilidades penales a este último […]».

2. Decreto de 5 de marzo de 2010

20. El Decreto de 5 de marzo de 2010, en su versión aplicable a los hechos del litigio principal, prevé, en su artículo 1:

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

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

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

[…]»

21. El artículo 4 de dicho Decreto establece:

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

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

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

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

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

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

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

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

22. El anexo del Decreto de 5 de marzo de 2010 dispone:

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

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

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

fecha y hora de los hechos;

dirección IP de los abonados afectados;

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

seudónimo utilizado por el abonado;

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

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

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

[…]

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

nombre y apellido;

dirección postal y direcciones electrónicas;

datos telefónicos;

dirección de la instalación de la línea telefónica del abonado;

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

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

[…]»

3. Código de Correos y Telecomunicaciones

23. El artículo L. 34-1 del Código de Correos y Comunicaciones Electrónicas, en su versión modificada por el artículo 17 de la Ley n.º 2021-998, de 30 de julio de 2021[5] (en lo sucesivo, «CPCE»), dispone, en su apartado II *bis*, que «los operadores de comunicaciones electrónicas están obligados a conservar:

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

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

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

III. Litigio principal, cuestiones prejudiciales y procedimiento ante el Tribunal de Justicia

24. Mediante recurso interpuesto el 12 de agosto de 2019 y dos escritos complementarios de 12 de noviembre de 2019 y de 6 de mayo de 2021, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net y French Data Network solicitan al Conseil d'État (Consejo de Estado) la anulación de la decisión tácita mediante la cual el Premier ministre (Primer Ministro, Francia) denegó su solicitud de derogación del Decreto de 5 de marzo de 2010, en la medida en que dicho Decreto y las disposiciones que constituyen su base jurídica no

[5] JORF de 31 de julio de 2021, texto n.º 1. Esta versión del artículo L. 34-1 del CPCE, en vigor desde el 31 de julio de 2021, fue adoptada a raíz de la decisión del Conseil d'État (Consejo de Estado) de 21 de abril de 2021, n.º 393099 (JORF de 25 de abril de 2021), por la que se descartó la versión anterior de dicha disposición, que incluía una obligación de conservación de datos personales «a efectos de la investigación, la comprobación y el enjuiciamiento de delitos o del incumplimiento de la obligación definida en el artículo L. 336-3 [del CPI]» con el único objetivo de permitir, de ser necesario, la puesta a disposición, en particular, de la Hadopi. Mediante decisión n.º 2021-976-977 QPC, de 25 de febrero de 2022 (Sr. Habib A. y otros), el Conseil constitutionnel (Consejo Constitucional, Francia) declaró que esta versión anterior del artículo L. 34-1 del CPCE era contraria a la Constitución por la razón esencial de que, «al autorizar la conservación general e indiferenciada de los datos de conexión, las disposiciones impugnadas vulneran el derecho al respeto de la vida privada en un grado desproporcionado» (apartado 13). En efecto, este órgano jurisdiccional consideró que los datos de conexión que deben conservarse en virtud de estas disposiciones no solo se refieren a la identificación de los usuarios de los servicios de comunicaciones electrónicas, sino también a otros datos que, «habida cuenta de su naturaleza, de su diversidad y del tratamiento al que pueden ser sometidos […] proporcionan una información abundante y precisa sobre estos usuarios y, en su caso, sobre terceros, que resulta especialmente intrusiva para su vida privada» (apartado 11).

solo vulneran indebidamente los derechos garantizados por la Constitución francesa, sino que también son contrarios al artículo 15 de la Directiva 2002/58, y a los artículos 7, 8, 11 y 52 de la Carta.

25. En particular, los recurrentes en el litigio principal alegan que el Decreto de 5 de marzo de 2010 y las disposiciones que constituyen su base jurídica autorizan el acceso a datos de conexión de forma desproporcionada por violaciones del derecho de autor cometidas en Internet y que no revisten gravedad, sin un control previo por parte de un juez o de una autoridad que ofrezca garantías de independencia e imparcialidad.

26. A este respecto, el órgano jurisdiccional remitente señala, en primer lugar, que el Tribunal de Justicia, en su última sentencia La Quadrature du Net y otros,[6] declaró que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a medidas legislativas que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia y de la protección de la seguridad pública, una conservación generalizada e indiferenciada *de los datos relativos a la identidad civil* de los usuarios de medios de comunicaciones electrónicas. Así, dicha conservación de tales datos es posible, sin ningún límite temporal concreto, a efectos de investigación, descubrimiento y enjuiciamiento de delitos en general.

27. El órgano jurisdiccional remitente deduce de ello que el motivo invocado por los recurrentes en el litigio principal relativo a la ilegalidad del Decreto de 5 de marzo de 2010, en la medida en que fue adoptado en el marco de la lucha contra las infracciones penales que no revisten gravedad, no puede sino desestimarse.

28. Dicho órgano jurisdiccional recuerda a continuación que el Tribunal de Justicia, en su sentencia Tele2 Sverige y Watson y otros,[7] declaró que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente.

29. Señala que el Tribunal de Justicia, en la sentencia Tele2,[8] especificó que, para garantizar en la práctica el pleno cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a la exigencia de un control previo de un órgano jurisdiccional o de una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se produzca a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, descubrimiento o acciones penales.

6 Véase la sentencia de 6 de octubre de 2020 (C-511/18, C-512/18 y C-520/18, en lo sucesivo, «sentencia La Quadrature du Net y otros», EU:C:2020:791), fallo.

7 Véase la sentencia de 21 de diciembre de 2016 (C-203/15 y C-698/15, en lo sucesivo, «sentencia Tele2», EU:C:2016:970), fallo.

8 Apartado 120 de dicha sentencia.

30. El órgano jurisdiccional remitente subraya que el Tribunal de Justicia recordó esa exigencia en la sentencia La Quadrature du Net y otros, [9] a propósito de la recogida en tiempo real de datos de conexión por los servicios de información, y en la sentencia Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), [10] que se refiere al acceso de las autoridades nacionales a los datos de conexión.

31. Ese órgano jurisdiccional observa, por último, que, desde su creación en 2009, se han remitido más de 12,7 millones de recomendaciones a los abonados, en virtud del procedimiento denominado de «respuesta gradual» previsto en el artículo L 331-25 del CPI, de las que 827 791 corresponden solo a 2019. Para ello, los agentes de la Comisión de Protección de los Derechos de la Hadopi deben ser capaces de recoger, cada año, una cantidad considerable de datos relativos a la identidad civil de los usuarios de que se trata. Considera que, dado el volumen de esas recomendaciones, el hecho de someter esa recogida a un control previo puede hacer imposible la aplicación de dichas recomendaciones.

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

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

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

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

33. Han presentado observaciones escritas los recurrentes en el litigio principal, los Gobiernos francés, estonio, sueco y noruego, así como la Comisión Europea. Estas mismas partes, a excepción del Gobierno estonio, y los Gobiernos danés y finlandés estuvieron representados en la vista que se celebró el 5 de julio de 2022.

[9] Apartado 189 de dicha sentencia.

[10] Sentencia de 2 de marzo de 2021 (C-746/18, en lo sucesivo, «sentencia Prokuratuur», EU:C:2021:152).

IV. Análisis

A. Sobre las cuestiones prejudiciales primera y segunda

34. Mediante sus cuestiones prejudiciales primera y segunda, que, a mi juicio, procede examinar conjuntamente, el órgano jurisdiccional remitente pretende que se dilucide, en esencia, si el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que permite, a una autoridad administrativa responsable de la protección de los derechos de autor y de los derechos afines frente a las violaciones de estos derechos cometidas en Internet, el acceso a los datos de identidad civil correspondientes a las direcciones IP con el fin de que dicha autoridad pueda identificar a los titulares de esas direcciones sospechosos de ser responsables de las referidas violaciones y pueda adoptar, en su caso, medidas contra ellos, sin que dicho acceso esté sujeto a un control previo por un órgano jurisdiccional o una entidad administrativa independiente.

1. Delimitación de las cuestiones prejudiciales

a) Recopilación previa de direcciones IP por parte de las organizaciones de titulares de derechos

35. De la resolución de remisión se desprende que el mecanismo de respuesta gradual controvertido en el litigio principal comprende dos operaciones sucesivas de tratamiento de datos que consisten, la primera, en la recopilación previa por parte de las organizaciones de titulares de derechos de las direcciones IP en las redes *peer-to-peer* de los infractores de los derechos de autor y, la segunda, en la vinculación de estas direcciones IP con la identidad civil de las personas por parte de la Hadopi una vez recibida la denuncia, con el fin de enviar recomendaciones a las personas cuyo acceso a los servicios de comunicación pública en línea ha sido utilizado infringiendo la normativa sobre los derechos de autor.

36. Las cuestiones prejudiciales primera y segunda se refieren únicamente a la segunda operación de tratamiento realizada por la Hadopi.

37. Sin embargo, los recurrentes en el litigio principal alegan que la primera operación de tratamiento debe ser objeto de examen por parte del Tribunal de Justicia, ya que, si esas direcciones IP se obtuvieron infringiendo las disposiciones de la Directiva 2002/58, su utilización en el marco de la segunda operación de tratamiento sería necesariamente contraria a dichas disposiciones.

38. Tal razonamiento no resulta convincente. El artículo 3, apartado 1, de la Directiva 2002/58 limita su ámbito de aplicación al «tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas». Sin embargo, como precisó el Gobierno francés en la vista, las organizaciones de titulares de derechos no obtienen las direcciones IP en cuestión a través de los proveedores de servicios de comunicación electrónica, sino directamente en línea, consultando los datos disponibles para el público en general.

39. Por lo tanto, no puede sino constatarse que la recopilación previa de las direcciones IP por las organizaciones de titulares de derechos no está comprendida en el ámbito de aplicación de las disposiciones de la Directiva 2002/58 y, como señala la Comisión, puede, en consecuencia,

analizarse a la luz de las disposiciones del Reglamento (UE) 2016/679.[11] Considero, en este sentido, que dicho análisis excede el marco de las cuestiones prejudiciales planteadas al Tribunal de Justicia, especialmente porque el órgano jurisdiccional remitente no aporta precisiones relativas a la recopilación previa que permitan al Tribunal de Justicia dar una respuesta útil.

40. En estas circunstancias, centraré mi análisis en la cuestión del acceso por parte de la Hadopi a los datos de identidad civil correspondientes a una dirección IP.

b) Vinculación de las direcciones IP con los datos de identidad civil

41. Las cuestiones prejudiciales primera y segunda atañen a «los datos de identidad civil correspondientes a una dirección IP», que son, según el órgano jurisdiccional remitente, de escasa sensibilidad. Dicho órgano jurisdiccional se refiere exclusivamente en su resolución a los apartados de la sentencia La Quadrature du Net y otros relativos a la conservación de los datos de identidad civil.

42. Es cierto que la jurisprudencia del Tribunal de Justicia traza una distinción entre el régimen de conservación de las direcciones IP y de acceso a estas direcciones y el régimen de conservación de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas y de acceso a estos datos, siendo este último menos estricto que el primero.[12]

43. Sin embargo, me parece que, en el presente asunto, a pesar de la formulación de ambas cuestiones prejudiciales, lo que está en juego no es el mero acceso a los datos de identidad civil de los usuarios de las comunicaciones electrónicas, sino la vinculación de estos datos a las direcciones IP de que dispone la Hadopi tras la recogida y transmisión de estas últimas por las organizaciones de titulares de derechos. En efecto, como señala la Comisión, el acceso a los datos de identidad civil por parte de la Hadopi tiene por objeto desbloquear un conjunto más amplio de datos, en particular las direcciones IP y los extractos de los archivos consultados, y permitir su explotación, ya que los datos de identidad civil y las direcciones IP no tienen, independientemente unos de otros, ningún interés para las autoridades nacionales, puesto que ni la identidad civil ni las direcciones IP pueden, por sí mismas, proporcionar información sobre las actividades de las personas físicas en línea cuando no están vinculadas entre sí.

44. En mi opinión, de ello se desprende que las cuestiones prejudiciales primera y segunda deben entenderse en el sentido de que no solo se refieren a los datos de identidad civil de los usuarios de un medio de comunicación electrónico, sino también al acceso a las direcciones IP que permiten identificar el origen de una conexión.

c) Conservación de las direcciones IP por parte de los proveedores de servicios de comunicación

45. Es cierto, como señalan el Gobierno francés y la Comisión, que las cuestiones prejudiciales planteadas al Tribunal de Justicia no se refieren formalmente a la conservación de datos por parte de los proveedores de servicios de comunicaciones electrónicas, sino únicamente al acceso de la Hadopi a los datos de identidad civil correspondientes a las direcciones IP.

[11] Reglamento 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).

[12] Véase la sentencia La Quadrature du Net y otros, apartados 155 y 159.

46. Sin embargo, la cuestión del acceso de la Hadopi a esos datos me parece en realidad inseparable de la cuestión previa de su conservación por parte de los proveedores de servicios de comunicaciones. Como ha señalado el Tribunal de Justicia, los datos solo se conservan con la finalidad de hacerlos accesibles, en su caso, a las autoridades nacionales competentes. [13] En otras palabras, la conservación de los datos y el acceso a estos no pueden entenderse de forma aislada, y ello aun cuando el segundo depende de la primera.

47. Es cierto que el Tribunal de Justicia ya ha examinado la compatibilidad con el artículo 15, apartado 1, de la Directiva 2002/58 de una normativa nacional relativa únicamente al acceso de las autoridades nacionales competentes a determinados datos personales, independientemente de la cuestión de la compatibilidad con dicha disposición de la conservación de los datos en cuestión. [14] Por lo tanto, las presentes cuestiones prejudiciales podrían responderse sin tener en cuenta si los datos en cuestión se han conservado de conformidad con las disposiciones del Derecho de la Unión.

48. Sin embargo, he de señalar, antes de nada, que en la sentencia Ministerio Fiscal, [15] el examen realizado por Tribunal de Justicia sobre la compatibilidad con el Derecho de la Unión del acceso de las autoridades nacionales a determinados datos personales se basa estrictamente en los mismos principios que el examen que realiza para evaluar la compatibilidad con el Derecho de la Unión de la conservación de dichos datos. En efecto, el Tribunal de Justicia se remite exclusivamente a la jurisprudencia desarrollada a este último respecto para extrapolarla a la cuestión del acceso a los datos personales. En otras palabras, a falta de un examen de la compatibilidad con el Derecho de la Unión de la conservación de determinados datos, dicho examen se pospone a la fase de la cuestión del acceso a esos datos, de modo que la compatibilidad de ese acceso depende en última instancia de la compatibilidad de la conservación.

49. A continuación, el Tribunal de Justicia ha indicado claramente que el acceso a los datos personales solo puede concederse para el caso de que esos datos hayan sido conservados por los proveedores de servicios de comunicaciones electrónicas de conformidad con el artículo 15, apartado 1, de la Directiva 2002/58 [16] y que el acceso a los datos personales por parte de los particulares para permitirles ejercer acciones ante la jurisdicción civil contra las infracciones al Derecho de propiedad intelectual solo es compatible con el Derecho de la Unión si dichos datos se conservan de forma compatible con dicha disposición. [17]

50. Por último, el Tribunal de Justicia ha declarado de forma reiterada que el acceso a los datos de tráfico y de localización conservados por los proveedores con arreglo a una medida adoptada de conformidad con el artículo 15, apartado 1, de la Directiva 2002/58, que debe efectuarse respetando los requisitos que se derivan de la jurisprudencia que ha interpretado la Directiva 2002/58, solo puede estar justificado, en principio, por el objetivo de interés general para el que dicha conservación se impuso a estos proveedores. [18] Dicho de otro modo, la compatibilidad con

[13] Véase la sentencia Tele2, apartado 79.

[14] Véase la sentencia de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), apartado 49.

[15] Sentencia de 2 de octubre de 2018 (C-207/16, EU:C:2018:788).

[16] Véase la sentencia Prokuratuur, apartado 29.

[17] Véase la sentencia de 17 de junio de 2021, M.I.C.M. (C-597/19, EU:C:2021:492), apartados 127 a 130.

[18] Véanse las sentencias La Quadrature du Net y otros, apartado 166; de 5 de abril de 2022, Commissioner of An Garda Síochána y otros (C-140/20, en lo sucesivo, «sentencia Commissioner of An Garda Síochána y otros», EU:C:2022:258), apartado 98, y de 20 de septiembre de 2022, SpaceNet y Telekom Deutschland, (C-793/19 y C-794/19, en lo sucesivo, «sentencia SpaceNet», EU:C:2022:702), apartado 131.

el Derecho de la Unión del acceso de las autoridades nacionales a determinados datos personales depende totalmente de la compatibilidad con el Derecho de la Unión de la conservación de estos datos.

51. De ello se desprende, en mi opinión, que el análisis de la compatibilidad con el Derecho de la Unión de una normativa nacional que prevé el acceso de una autoridad nacional a los datos personales presupone que se haya establecido previamente si la conservación de esos datos es compatible con el Derecho de la Unión.

52. En estas circunstancias, comenzaré mi análisis recordando la jurisprudencia del Tribunal de Justicia relativa a la cuestión de la conservación de las direcciones IP atribuidas al origen de una conexión, con el fin de demostrar sus límites y proponer una interpretación ajustada de la normativa en cuestión.

2. Jurisprudencia del Tribunal de Justicia relativa a la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 en relación con las medidas de conservación de las direcciones IP atribuidas al origen de una conexión

53. El artículo 5, apartado 1, de la Directiva 2002/58 consagra el principio de confidencialidad tanto de las comunicaciones electrónicas como de los datos de tráfico asociados a ellas, e implica, en particular, la prohibición, en principio, de que cualquier persona distinta de los usuarios almacene esas comunicaciones y datos sin el consentimiento de estos. [19]

54. Por lo que se refiere al tratamiento y almacenamiento por parte de los proveedores de servicios de comunicaciones electrónicas de los datos de tráfico relativos a abonados y usuarios, la Directiva 2002/58 establece, en su artículo 6, apartado 1, que esos datos deberán eliminarse o hacerse anónimos cuando ya no sean necesarios para la transmisión de una comunicación e indica, en su artículo 6, apartado 2, que podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones solamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. En cuanto a los datos de localización distintos de los datos de tráfico, el artículo 9, apartado 1, de dicha Directiva establece que esos datos solo podrán tratarse en ciertas condiciones, si se hacen anónimos, o previo consentimiento de los usuarios o abonados. [20]

55. Así pues, al adoptar la Directiva 2002/58, el legislador de la Unión concretó los derechos consagrados en los artículos 7 y 8 de la Carta, de modo que los usuarios de los medios de comunicaciones electrónicas tienen derecho a contar con que, en principio, de no mediar su consentimiento, sus comunicaciones y los datos relativos a ellas permanezcan anónimos y no puedan registrarse. [21] Por lo tanto, dicha Directiva no se limita a regular el acceso a tales datos mediante garantías dirigidas a prevenir los abusos, sino que también consagra, en particular, el principio de prohibición de su almacenamiento por terceros.

[19] Véanse las sentencias La Quadrature du Net y otros, apartado 107; Commissioner of An Garda Síochána y otros, apartado 35, y SpaceNet, apartado 52.

[20] Véanse las sentencias Tele2, apartado 86; La Quadrature du Net y otros, apartado 108; Commissioner of An Garda Síochána y otros, apartado 38, y SpaceNet, apartado 55.

[21] Véanse las sentencias La Quadrature du Net y otros, apartado 109; Commissioner of An Garda Síochána y otros, apartado 37, y SpaceNet, apartado 54.

56. En estas circunstancias, en la medida en que el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros adoptar medidas legales para «limitar el alcance» de los derechos y las obligaciones que se establecen en particular en los artículos 5, 6 y 9 de dicha Directiva, como los derivados de los principios de confidencialidad de las comunicaciones y de prohibición de almacenamiento de los datos asociados a ellas, tal disposición introduce una excepción a la regla general establecida, en particular, en dichos artículos 5, 6 y 9, por lo que, conforme a reiterada jurisprudencia, debe ser objeto de una interpretación estricta. En consecuencia, tal disposición no puede justificar que la excepción a la obligación de principio de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos relativos a ellas y, en particular, a la prohibición de almacenar esos datos, prevista en el artículo 5 de la citada Directiva, se convierta en la regla si no se quiere privar en gran medida a esta última disposición de su alcance [22]

57. Por lo que respecta a los objetivos que pueden justificar una limitación de los derechos y de las obligaciones previstos, en particular, en los artículos 5, 6 y 9 de la Directiva 2002/58, el Tribunal de Justicia ya ha declarado que la enumeración de los objetivos que figuran en el artículo 15, apartado 1, primera frase, de dicha Directiva tiene carácter exhaustivo, de modo que la medida legislativa que se adopte en virtud de esta disposición ha de responder efectiva y estrictamente a uno de ellos. [23]

58. Además, del artículo 15, apartado 1, tercera frase, de la Directiva 2002/58 se infiere que las medidas adoptadas por los Estados miembros con arreglo a esta disposición deben respetar los principios generales del Derecho de la Unión, entre los que figura el principio de proporcionalidad, y los derechos fundamentales garantizados por la Carta. A este respecto, el Tribunal de Justicia ya ha declarado que la obligación impuesta por un Estado miembro a los proveedores de servicios de comunicaciones electrónicas, mediante una normativa nacional, de conservar los datos de tráfico con el fin de hacerlos accesibles, en su caso, a las autoridades nacionales competentes suscita dudas en cuanto al cumplimiento no solo de los artículos 7 y 8 de la Carta, relativos a la protección de la vida privada y a la protección de datos de carácter personal, respectivamente, sino también del artículo 11 de la Carta, relativo a la libertad de expresión, libertad que constituye uno de los fundamentos esenciales de una sociedad democrática y pluralista, y forma parte de los valores en los que se basa la Unión Europea, con arreglo al artículo 2 TUE. [24]

59. Ahora bien, en la medida en que el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros limitar los derechos y las obligaciones previstos en los artículos 5, 6 y 9 de dicha Directiva, esta disposición refleja el hecho de que los derechos consagrados en los artículos 7, 8 y 11 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse de acuerdo con su función en la sociedad. En efecto, como se desprende de su artículo 52, apartado 1, la Carta admite limitaciones al ejercicio de esos derechos, siempre que se establezcan por ley, respeten el contenido esencial de los citados derechos y, ajustándose al principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás. De este modo, la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 a la luz de la Carta exige tener en cuenta asimismo la importancia que presentan los objetivos de

[22] Véanse las sentencias La Quadrature du Net y otros, apartados 110 y 111; Commissioner of An Garda Síochána y otros, apartado 40, y SpaceNet, apartado 57.

[23] Véanse las sentencias La Quadrature du Net y otros, apartado 112; Commissioner of An Garda Síochána y otros, apartado 41, y SpaceNet, apartado 58.

[24] Véanse las sentencias La Quadrature du Net y otros, apartados 113 y 114; Commissioner of An Garda Síochána y otros, apartado 42, y SpaceNet, apartado 60.

protección de la seguridad nacional y de lucha contra la delincuencia grave al contribuir a la protección de los derechos y de las libertades de terceros y de los derechos consagrados en los artículos 3, 4, 6 y 7 de la Carta, [25] de los que pueden resultar obligaciones positivas que incumban a los poderes públicos. [26]

60. En consecuencia, frente a estas diferentes obligaciones positivas, conviene proceder a una conciliación de los distintos intereses legítimos y derechos en juego. En este marco, de los propios términos del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 se infiere que los Estados miembros podrán adoptar una medida que suponga una excepción al principio de confidencialidad cuando tal medida sea «necesaria, proporcionada y apropiada en una sociedad democrática», mientras que el considerando 11 de esta Directiva precisa a tal efecto que una medida de esta naturaleza debe ser «rigurosamente» proporcionada al objetivo que pretende lograr. [27]

61. A este respecto, de la jurisprudencia del Tribunal de Justicia se desprende que la posibilidad de que los Estados miembros justifiquen una limitación de los derechos y obligaciones previstos, en particular, en los artículos 5, 6 y 9 de la Directiva 2002/58 debe apreciarse determinando la gravedad de la injerencia que supone esa limitación y comprobando que la importancia del objetivo de interés general perseguido por dicha limitación guarde relación con tal gravedad. [28]

62. Por otra parte, he de señalar que el Tribunal de Justicia distingue en su jurisprudencia entre, por una parte, las injerencias resultantes del acceso a datos que, como tales, proporcionan información precisa sobre las comunicaciones en cuestión y, por lo tanto, sobre la vida privada de la persona, y cuyo régimen de conservación es estricto, y, por otra parte, las injerencias resultantes del acceso a datos que solo pueden proporcionar dicha información en la medida en que están vinculados a otros datos, como las direcciones IP. [29]

63. Así, por lo que se refiere más concretamente a las direcciones IP, el Tribunal de Justicia declaró que estas se generan sin estar vinculadas a una comunicación determinada y sirven fundamentalmente para identificar, por medio de los proveedores de servicios de comunicaciones electrónicas, a la persona física propietaria de un equipo terminal desde el que se efectúa una comunicación a través de Internet. Por lo tanto, dado que las únicas direcciones IP que se conservan son las del origen de la comunicación y no las de su destinatario, esta categoría de datos presenta un grado de sensibilidad menor que los demás datos de tráfico. [30]

64. Al mismo tiempo, el Tribunal de Justicia subraya que, puesto que estas direcciones pueden utilizarse para llevar a cabo, en particular, el rastreo exhaustivo de la secuencia de navegación de un internauta y, en consecuencia, de su actividad en línea, tales datos permiten establecer el perfil detallado de este y extraer conclusiones precisas sobre la vida privada del usuario. Por lo tanto, la

[25] Véanse las sentencias La Quadrature du Net y otros, apartados 120 y 122; Commissioner of An Garda Síochána y otros, apartado 48, y SpaceNet, apartado 63.

[26] Véanse las sentencias La Quadrature du Net y otros, apartados 120 y 122; Commissioner of An Garda Síochána y otros, apartado 49, y SpaceNet, apartado 64.

[27] Véanse las sentencias La Quadrature du Net y otros, apartados 127 y 129; Commissioner of An Garda Síochána y otros, apartados 50 y 51, y SpaceNet, apartados 65 y 66.

[28] Véanse las sentencias La Quadrature du Net y otros, apartado 131; Commissioner of An Garda Síochána y otros, apartado 53, y SpaceNet, apartado 68.

[29] Véanse los puntos 41 y ss. de las presentes conclusiones.

[30] Véase la sentencia La Quadrature du Net y otros, apartado 152.

conservación y el análisis de dichas direcciones IP constituyen injerencias *graves* en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, y pueden tener efectos disuasorios sobre el ejercicio de la libertad de expresión garantizada en el artículo 11 de la Carta. [31]

65. No obstante, según reiterada jurisprudencia, a efectos de la necesaria conciliación de los derechos y de los intereses legítimos en cuestión exigida por la jurisprudencia, debe tenerse en cuenta el hecho de que, en caso de un delito cometido en línea, la dirección IP puede constituir el único método de investigación para identificar a la persona a la que se atribuyó esa dirección en el momento en que se cometió dicha infracción penal. [32]

66. Por consiguiente, el Tribunal de Justicia considera que una medida legislativa que establece únicamente la conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión no parece, en principio, contraria al artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, siempre que esta posibilidad esté sujeta al riguroso respeto de las condiciones materiales y procesales que deben regular la utilización de tales datos y partiendo de la base de que, habida cuenta del carácter grave de la injerencia que supone esta conservación, solo la lucha contra la *delincuencia grave* y la prevención de las amenazas graves a la seguridad pública pueden, al igual que la protección de la seguridad nacional, justificar esta injerencia. [33]

67. El Tribunal de Justicia precisa además que la duración del período de conservación no puede exceder de lo estrictamente necesario habida cuenta del objetivo perseguido y que una medida de esta naturaleza debe prever condiciones y garantías estrictas por lo que se refiere a la explotación de dichos datos. [34]

3. Límites de la jurisprudencia relativa a la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 en relación con las medidas de conservación de las direcciones IP atribuidas al origen de una conexión

68. No obstante, considero que la solución a la que ha llegado el Tribunal de Justicia en relación con las medidas nacionales de conservación de las direcciones IP atribuidas al origen de una conexión, interpretada a la luz del artículo 15, apartado 1, de la Directiva 2002/58, presenta dos dificultades principales.

a) Conciliación con la jurisprudencia sobre la comunicación de las direcciones IP atribuidas al origen de una conexión en el marco de recursos para la protección de los derechos de propiedad intelectual

69. En primer lugar, como ya he mencionado en mis conclusiones presentadas en el asunto M.I.C.M., [35] existe una cierta tensión entre esta línea jurisprudencial y la relativa a la comunicación de las direcciones IP en el marco de recursos para la protección de los derechos de

[31] Véanse las sentencias La Quadrature du Net y otros, apartado 153; Commissioner of An Garda Síochána y otros, apartado 73, y SpaceNet, apartado 103 (el subrayado es mío).

[32] Véanse las sentencias La Quadrature du Net y otros, apartado 154; Commissioner of An Garda Síochána y otros, apartado 73, y SpaceNet, apartado 103.

[33] Véanse las sentencias La Quadrature du Net y otros, apartados 155 y 156; Commissioner of An Garda Síochána y otros, apartado 74, y SpaceNet, apartados 104 y 105 (el subrayado es mío).

[34] Véanse las sentencias La Quadrature du Net y otros, apartado 156, y SpaceNet, apartado 105.

[35] C-597/19, EU:C:2020:1063, punto 98.

propiedad intelectual a los titulares de los mismos, que hace hincapié en la obligación de los Estados miembros de garantizar que los titulares de los derechos de propiedad intelectual tengan posibilidades reales de obtener una reparación de los daños y perjuicios resultantes de las vulneraciones de tales derechos. [36]

70. En efecto, por lo que respecta a esta segunda línea jurisprudencial, el Tribunal de Justicia ha declarado reiteradamente que el Derecho de la Unión no se opone a que los Estados miembros establezcan una obligación de transmitir a particulares datos personales para permitir ejercer acciones ante la jurisdicción civil contra las infracciones al Derecho de propiedad intelectual. [37]

71. El Tribunal de Justicia señala, a este respecto, que la posibilidad de que los Estados miembros impongan el deber de divulgar datos personales en un procedimiento civil se deprende, antes de nada, de la posibilidad de imponer tal divulgación en el marco de la persecución de infracciones penales, que, a continuación, se ha ampliado a los procedimientos civiles. [38]

72. Sin embargo, al mismo tiempo, en lo que respecta a las direcciones IP, el Tribunal de Justicia impone que estos datos solo pueden conservarse en el marco de la lucha contra la delincuencia grave y la prevención de las amenazas graves a la seguridad pública. [39]

73. Los intentos de conciliar estas dos líneas jurisprudenciales conducen, en mi opinión, a resultados inadecuados y no resultan convincentes.

74. Por una parte, contrariamente a lo que alegó el Gobierno francés en la vista, la lucha contra las violaciones de los derechos de propiedad intelectual no puede entrar en el ámbito de la lucha contra la delincuencia grave. El concepto de «delincuencia grave» debe, en mi opinión, recibir una interpretación autónoma. Esta no puede depender de los conceptos de cada Estado miembro, puesto que ello permitiría eludir los requisitos del artículo 15, apartado 1, de la Directiva 2002/58 en función de que los Estados miembros adopten un concepto amplio o no de la lucha contra la delincuencia grave. Ahora bien, como ya he señalado, los intereses relativos a la protección de los derechos de propiedad intelectual no pueden confundirse con los que subyacen a la lucha contra la delincuencia grave. [40]

75. Por otra parte, permitir la transmisión de las direcciones IP a los titulares de derechos de propiedad intelectual en el marco de los procedimientos que tienen por objeto la protección de tales derechos, aun cuando su conservación solo sea posible en el contexto de la lucha contra la delincuencia grave, sería claramente contrario a la jurisprudencia del Tribunal de Justicia sobre la conservación de los datos de conexión y equivaldría a privar de todo efecto útil a las condiciones exigidas para la conservación de dichos datos, ya que, en cualquier caso, se podría acceder a ellos con fines diferentes.

76. De ello se desprende, a mi modo de ver, que la conservación de las direcciones IP a efectos de la protección de los derechos de propiedad intelectual y su comunicación a los titulares de esos derechos en el marco de los procedimientos que tienen por objeto dicha protección podrían ser contrarias al artículo 15, apartado 1, de la Directiva 2002/58, tal como lo interpreta la

36 Véanse mis conclusiones presentadas en el asunto M.I.C.M. (C-597/19, EU:C:2020:1063), punto 97.

37 Véanse las sentencias de 19 de abril de 2012, Bonnier Audio y otros (C-461/10, EU:C:2012:219), apartado 55; de 4 de mayo de 2017, Rīgas satiksme (C-13/16, EU:C:2017:336), apartado 34, y de 17 de junio de 2021, M.I.C.M. (C-597/19, EU:C:2021:492), apartados 47 a 54.

38 Véase, en este sentido, la sentencia de 29 de enero de 2008, Promusicae (C-275/06, EU:C:2008:54), apartados 50 a 52.

39 Véase el punto 65 de las presentes conclusiones.

40 Véanse mis conclusiones presentadas en el asunto M.I.C.M. (C-597/19, EU:C:2020:1063), punto 103.

jurisprudencia del Tribunal de Justicia. La obligación de transmitir a particulares datos personales para permitir ejercer acciones ante la jurisdicción civil contra las infracciones al Derecho de propiedad intelectual, posible gracias al propio Tribunal de Justicia, queda al mismo tiempo neutralizada por su propia jurisprudencia sobre la conservación de las direcciones IP por parte de los proveedores de servicios de comunicaciones electrónicas.

77. Sin embargo, esta solución es insatisfactoria en la medida en que pondría en entredicho el equilibrio que el Tribunal de Justicia pretendía establecer entre los distintos intereses en juego, al privar a los titulares de derechos de propiedad intelectual del principal, si no único, medio de identificación de los autores de las violaciones de esos derechos en línea. Esta consideración me lleva a exponer la segunda dificultad que, a mi juicio, puede plantear la jurisprudencia del Tribunal de Justicia en relación con las medidas nacionales de conservación de las direcciones IP atribuidas al origen de una conexión interpretada a la luz del artículo 15, apartado 1, de la Directiva 2002/58.

b) Riesgo de impunidad sistémica para las infracciones penales cometidas exclusivamente en línea

78. Así, en segundo lugar, considero que esta solución da lugar a una serie de dificultades prácticas. Como señala el propio Tribunal de Justicia, en el caso de una infracción penal cometida exclusivamente en línea, la dirección IP puede constituir el único método de investigación para identificar a la persona a la que se atribuyó esa dirección en el momento en que se cometió.

79. Sin embargo, me parece que este elemento no se tiene plenamente en cuenta en la ponderación de los intereses en juego. Dado que el Tribunal de Justicia limita no obstante la posibilidad de conservar direcciones IP a la lucha contra la delincuencia grave, excluye al mismo tiempo que esos datos puedan conservarse para luchar contra las infracciones penales en general, a pesar de que algunas de estas solo pueden prevenirse, detectarse o castigarse gracias a dichos datos.

80. En otras palabras, la jurisprudencia del Tribunal de Justicia puede llevar a privar a las autoridades nacionales del único medio de identificación de los autores de delitos en línea que, sin embargo, no son delitos graves, como las violaciones de los derechos de propiedad intelectual. De hecho, esto daría lugar a una impunidad sistémica para los delitos cometidos exclusivamente en línea, y no solo para las violaciones de los derechos de propiedad intelectual. Pienso, en particular, en los actos de difamación cometidos en línea. El Derecho de la Unión prevé ciertamente el derecho de obtener un requerimiento judicial contra los intermediarios cuyos servicios son usados para cometer tales violaciones,[41] pero podría resultar de la jurisprudencia del Tribunal de Justicia que los propios autores de esos actos nunca podrían ser perseguidos.

81. A menos que se acepte que toda una serie de delitos no puedan ser nunca perseguidos, considero que procede analizar de nuevo el equilibrio entre los diferentes intereses implicados.

82. Estas distintas consideraciones me llevan a proponer al Tribunal de Justicia una cierta adaptación de la jurisprudencia relativa a las medidas nacionales de conservación de las direcciones IP interpretadas a la luz del artículo 15, apartado 1, de la Directiva 2002/58.

[41] Artículo 15, apartado 1, de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO 2000, L 178, p. 1).

4. Propuesta de adaptación de la jurisprudencia del Tribunal de Justicia relativa a la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 en lo que respecta a las medidas de conservación de las direcciones IP atribuidas al origen de una conexión

83. A la luz de las consideraciones anteriores, soy de la opinión de que el artículo 15, apartado 1, de la Directiva 2002/58 debe interpretarse en el sentido de que no se opone a las medidas que prevén la conservación general e indiferenciada de las direcciones IP atribuidas al origen de una conexión, durante un período de tiempo limitado al mínimo estrictamente necesario, a efectos de garantizar la prevención, investigación, descubrimiento y enjuiciamiento de delitos en línea respecto de los que la dirección IP constituye *el único método* de investigación para identificar a la persona a la que se atribuyó esa dirección en el momento en que se cometió el delito.

84. Debo subrayar a este respecto que tal propuesta no cuestiona, en mi opinión, la exigencia de proporcionalidad impuesta a la conservación de datos, habida cuenta del carácter grave de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que dicha injerencia supone. [42] Por el contrario, cumple plenamente este requisito.

85. Por una parte, la limitación de los derechos y obligaciones previstos en los artículos 5, 6 y 9 de la Directiva 2002/58 que constituye la conservación de direcciones IP persigue un objetivo de interés general en relación con dicha gravedad, a saber, la prevención, investigación, descubrimiento y enjuiciamiento de delitos contemplados en los textos, que de otro modo quedarían sin efecto.

86. Por otro lado, esta limitación tiene lugar dentro de los límites de lo estrictamente necesario. De hecho, dicha conservación se limita a casos específicos, a saber, delitos cometidos en línea y cuyo autor solo puede ser identificado a través de la dirección IP que se le ha asignado. En otras palabras, no se trata de permitir una conservación de datos general e indiferenciada sin más condiciones, sino solo de hacer posible el enjuiciamiento de delitos concretos, no de delitos en general.

87. Sin embargo, aunque el artículo 15, apartado 1, de la Directiva 2002/58 no se opone a una conservación general e indiferenciada de las direcciones IP atribuidas al origen de una conexión a efectos de garantizar la prevención, investigación, descubrimiento y enjuiciamiento de delitos en línea respecto de los que la dirección IP constituye el único método de investigación para identificar a la persona a la que se atribuyó esa dirección en el momento en que se cometió dicho delito, conviene precisar asimismo que, según la jurisprudencia, esta posibilidad debe estar sujeta «al riguroso respeto de las condiciones materiales y procesales *que deben regular la utilización de tales datos*». [43] El Tribunal de Justicia también especifica que dicha medida «debe prever condiciones y garantías estrictas por lo que se refiere a *la explotación de dichos datos*». [44]

88. En otras palabras, como ya he señalado, la conservación de los datos y el acceso a estos no pueden entenderse de forma aislada. En estas circunstancias, si bien la posibilidad de que la Hadopi acceda a las direcciones IP no es de entrada contraria al artículo 15, apartado 1, de la Directiva 2002/58, en la medida en que dichos datos se conservaron de conformidad con los requisitos establecidos en dicha disposición, sigue siendo necesario, para responder a las cuestiones prejudiciales planteadas al Tribunal de Justicia, examinar si las condiciones de acceso

[42] Puntos 60 y 61 de las presentes conclusiones.

[43] Véase la sentencia La Quadrature du Net y otros, apartado 155 (el subrayado es mío).

[44] Véase la sentencia La Quadrature du Net y otros, apartado 156 (el subrayado es mío).

a las direcciones IP atribuidas al origen de una conexión por la Hadopi son, en sí mismas, conformes a dicha disposición, en particular en lo que respecta a la necesidad o no de un control previo por un órgano jurisdiccional o una autoridad administrativa independiente.

89. Una vez analizada la cuestión preliminar de la conservación de las direcciones IP atribuidas al origen de una conexión, procederé a examinar el acceso de la Hadopi a estos datos a la luz del artículo 15, apartado 1, de la Directiva 2002/58.

5. Acceso a los datos de identidad civil correspondientes a las direcciones IP por parte de la Hadopi

90. De la jurisprudencia del Tribunal de Justicia se desprende, en lo que respecta a los objetivos que pueden justificar una medida nacional de excepción al principio de confidencialidad de las comunicaciones electrónicas, que el acceso a los datos debe responder estricta y objetivamente a uno de esos objetivos, y que el objetivo perseguido por dicha medida debe guardar relación con la gravedad de la injerencia en los derechos fundamentales que dicho acceso supone. [45]

91. Además, como ya he explicado, [46] el acceso a los datos conservados por los proveedores con arreglo a una medida adoptada de conformidad con el artículo 15, apartado 1, de la Directiva 2002/58 solo puede estar justificado, en principio, por el objetivo de interés general para el que dicha conservación se impuso a estos proveedores. [47]

92. Así, el Tribunal de Justicia consideró, conforme al principio de proporcionalidad, que, en el ámbito de la prevención, investigación, descubrimiento y enjuiciamiento de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de grave. [48]

93. A este respecto, he de señalar, contrariamente a lo que sostienen el Gobierno francés y la Comisión, que el acceso de la Hadopi a los datos de identidad civil correspondientes a una dirección IP sí constituye una injerencia grave en los derechos fundamentales. En efecto, no se trata simplemente de acceder a los datos de identidad civil, que son, en sí mismos, de escasa sensibilidad, sino de vincular esos datos a un conjunto más amplio de datos, a saber, la dirección IP, y también, como señalan los recurrentes en el litigio principal, un extracto del archivo descargado vulnerando los derechos de autor. Se trata, por lo tanto, de vincular la identidad civil de una persona al contenido del archivo consultado y a la dirección IP a través de la cual se ha realizado dicha consulta.

94. Sin embargo, al igual que abogo por permitir asimismo la conservación de datos que constituye una injerencia grave en los derechos fundamentales a efectos de garantizar la prevención, investigación, descubrimiento y enjuiciamiento de delitos en línea respecto de los que la dirección IP constituye el único método de investigación para identificar a la persona a la que se atribuyó esa dirección en el momento en que se cometió el delito, [49] creo que debería posibilitarse el acceso a esos datos para perseguir el mismo objetivo, salvo que se acepte la impunidad general de los delitos cometidos exclusivamente en línea.

[45] Véanse las sentencias de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), apartado 55, y Prokuratuur, apartado 32.

[46] Punto 47 de las presentes conclusiones.

[47] Véanse las sentencias SpaceNet, apartado 131; La Quadrature du Net y otros, apartado 166, y Commissioner of An Garda Síochána y otros, apartado 98.

[48] Véanse las sentencias Tele2, apartado 115; de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), apartado 56, y Prokuratuur, apartado 33.

[49] Véanse los puntos 65 y ss. de las presentes conclusiones.

95. Por lo tanto, el acceso de la Hadopi a los datos de identidad civil vinculados a una dirección IP me parece justificado por el objetivo de interés general por el que se impuso esa conservación a los proveedores de servicios de comunicaciones electrónicas.

96. No obstante, la jurisprudencia del Tribunal de Justicia aclara que una normativa nacional que regula el acceso de las autoridades competentes a los datos de tráfico y de localización conservados no puede limitarse a exigir que el acceso responda a la finalidad perseguida por dicha normativa, sino que debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos en cuestión. [50]

97. En particular, el Tribunal de Justicia declara que, puesto que un acceso general a todos los datos conservados, con independencia de la existencia de una relación con el fin perseguido, no puede considerarse limitado a lo estrictamente necesario, la normativa nacional debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos de los usuarios, de modo que se compruebe que el acceso únicamente se conceda a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave. [51]

98. Así, según la jurisprudencia, para garantizar en la práctica el íntegro cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados se supedite, en principio, a un control previo efectuado, bien por un órgano jurisdiccional, bien por un órgano administrativo independiente. [52]

99. Sin embargo, he de señalar que el Tribunal de Justicia ha establecido esta necesidad de control previo del acceso a los datos personales en circunstancias particulares que difieren del presente asunto, que implican intrusiones *especialmente graves* en la vida privada de los usuarios de los servicios de comunicaciones electrónicas.

100. En efecto, cada una de las sentencias que subrayaron este requisito se refería a medidas nacionales por las que se autorizaba el acceso al conjunto de los datos relativos al tráfico y a la localización de los usuarios relativos a todos los medios de comunicación electrónica [53] o, al menos, a la telefonía fija y móvil. [54] Más concretamente, se trataba del acceso a un «conjunto de datos […] que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y permitir extraer conclusiones precisas sobre su vida privada», [55] de modo que la exigencia de un control previo del acceso a tales datos por un órgano jurisdiccional o una entidad administrativa independiente solo existe, a mi juicio, en estas condiciones.

101. Pues bien, por una parte, el acceso de la Hadopi se limita a vincular los datos de identidad civil a la dirección IP utilizada y al archivo consultado en un momento determinado, sin permitir a las autoridades competentes reconstruir la secuencia de navegación en línea del usuario de que

50 Véanse las sentencias Tele2, apartado 118; Prokuratuur, apartado 49, y Commissioner of An Garda Síochána y otros, apartado 104.

51 Véanse las sentencias Tele2, apartado 119; Prokuratuur, apartado 50, y Commissioner of An Garda Síochána y otros, apartado 105.

52 Véanse las sentencias Tele2, apartado 120; Prokuratuur, apartado 51, y Commissioner of An Garda Síochána y otros, apartado 106.

53 Véanse las sentencias Tele2 y Commissioner of An Garda Síochána y otros.

54 Véase la sentencia Prokuratuur.

55 Véase la sentencia Prokuratuur, apartado 45.

se trate ni, por consiguiente, extraer conclusiones precisas sobre su vida privada más allá del conocimiento del archivo concreto consultado en el momento de la infracción penal. No se trata, pues, de permitir el rastreo de todas las actividades en línea del usuario en cuestión.

102. Por otra parte, estos datos solo se refieren a los datos de las personas que, según consta en las actas levantadas por las organizaciones de titulares de derechos, han cometido hechos que puedan constituir un incumplimiento de la obligación prevista en el artículo L. 336-3 del CPI. Por lo tanto, el acceso de la Hadopi a los datos de identidad civil vinculados a las direcciones IP se limita estrictamente a lo necesario para alcanzar el objetivo perseguido, a saber, permitir la prevención, investigación, descubrimiento y enjuiciamiento de delitos en línea respecto de los que la dirección IP constituye el único método de investigación para identificar a la persona a la que se atribuyó esa dirección en el momento en que se cometió dicho delito, en el que se inscribe el mecanismo de respuesta gradual.

103. En estas circunstancias, considero que el artículo 15, apartado 1, de la Directiva 2002/58 no exige la existencia de un control previo del acceso de la Hadopi a los datos de identidad civil vinculados a las direcciones IP de los usuarios por un órgano jurisdiccional o una entidad administrativa independiente.

104. Por lo demás, observo, como señala el Gobierno francés, que el acceso de la Hadopi a estos datos, si bien no está sometido a un control previo por un órgano jurisdiccional o una entidad administrativa independiente, no está exento de todo control, ya que el fichero enviado por la Hadopi a los operadores de comunicaciones electrónicas es elaborado cada día por un agente jurado a partir de las denuncias recibidas y validadas, de forma aleatoria por muestreo, antes de ser añadidas al fichero. [56] Ante todo, procede observar que el procedimiento de respuesta gradual sigue estando sujeto a las disposiciones de la Directiva (UE) 2016/680. [57] En este sentido, las personas físicas a las que se dirige la Hadopi disfrutan de un conjunto de garantías materiales y procesales previstas por esta Directiva. Estos incluyen el derecho de acceso, rectificación y supresión de los datos personales tratados por la Hadopi, así como la posibilidad de presentar una reclamación ante una autoridad administrativa independiente, seguida, en su caso, de un recurso judicial interpuesto con arreglo a las condiciones de Derecho común. [58]

105. Por lo tanto, propongo responder a las cuestiones prejudiciales primera y segunda que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que no se opone a una normativa nacional que permite a los proveedores de servicios de comunicaciones electrónicas la conservación de los datos de identidad civil correspondientes a las direcciones IP y a una autoridad administrativa responsable de la protección de los derechos de autor y de los derechos afines frente a las violaciones de estos derechos cometidas en Internet el acceso limitado a tales

[56] Con carácter accesorio, he de señalar que las alegaciones de viabilidad también se oponen a la obligación de realizar un control previo sistemático. La existencia de un sistema organizado de lucha contra las violaciones de los derechos de autor cometidas en línea, como el controvertido en el litigio principal, presupone la necesidad de tratar grandes cantidades de datos personales, proporcionales al número de violaciones perseguidas, a saber, a modo de ejemplo para el año 2019, según las observaciones del Gobierno francés, 33 465 solicitudes de identificación de direcciones IP realizadas por la Hadopi al día. En este contexto, la obligación de realizar un control previo del acceso a estos datos podría socavar, en la práctica, el funcionamiento de los mecanismos organizados de lucha contra la vulneración de derechos de propiedad intelectual en línea, poniendo en tela de juicio el equilibrio entre los derechos de los usuarios y los de los autores.

[57] Directiva del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89).

[58] Todas estas garantías están previstas en las disposiciones del capítulo III, título III, de la Ley n.º 78-17, relativa a la Informática, los Archivos y las Libertades, de 6 de enero de 1978 (JORF de 7 de enero de 1978).

datos con el fin de que dicha autoridad pueda identificar a los titulares de esas direcciones sospechosos de ser responsables de las referidas violaciones y pueda adoptar, en su caso, medidas contra ellos, sin que dicho acceso esté sujeto a un control previo por un órgano jurisdiccional o una entidad administrativa independiente, cuando dichos datos constituyen el único método de investigación para identificar a la persona que tenía atribuida esa dirección en el momento en que se cometió la infracción penal.

B. Sobre la tercera cuestión prejudicial

106. Mediante su tercera cuestión prejudicial, el órgano jurisdiccional remitente pretende que se dilucide si, en caso de respuesta afirmativa a las cuestiones prejudiciales primera y segunda, y a la vista de la escasa sensibilidad de los datos de identidad civil, del marco estricto de acceso a los datos y del imperativo de no poner en peligro el cumplimiento de la misión de servicio público conferida a la autoridad administrativa de que se trata, el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a que el control previo del acceso se efectúe conforme a modalidades adaptadas, tales como un control automatizado, en su caso bajo la supervisión de un servicio interno del organismo que ofrezca garantías de independencia e imparcialidad en relación con los agentes encargados de realizar esta recogida.

107. Del tenor de la tercera cuestión prejudicial y de la respuesta escrita del Gobierno francés a las preguntas del Tribunal de Justicia se desprende que las modalidades de control adaptadas a las que se refiere dicha cuestión no aluden a un mecanismo de control existente en el Derecho nacional, sino a las vías que pueden explorarse y que tienen por objeto adecuar, en su caso, el mecanismo francés al Derecho de la Unión.

108. Ahora bien, constituye jurisprudencia reiterada que una petición de decisión prejudicial no tiene como objetivo la formulación de opiniones consultivas sobre cuestiones generales o hipotéticas, sino que busca satisfacer la necesidad inherente a la solución efectiva de un litigio relativo al Derecho de la Unión. [59]

109. Por lo tanto, en la medida en que la tercera cuestión prejudicial tiene, en mi opinión, carácter hipotético, debe ser declarada inadmisible.

110. En todo caso, a la vista de la respuesta que propongo que se dé a las cuestiones prejudiciales primera y segunda, no me parece necesario responder a la tercera cuestión prejudicial.

[59] Véanse las sentencias de 26 de octubre de 2017, Balgarska energiyna borsa (C-347/16, EU:C:2017:816), apartado 31; de 31 de mayo de 2018, Confetra y otros (C-259/16 y C-260/16, EU:C:2018:370), apartado 63, y de 17 de octubre de 2019, Elektrorazpredelenie Yug (C-31/18, EU:C:2019:868), apartado 32.

V. Conclusión

111. Habida cuenta del conjunto de consideraciones anteriores, propongo al Tribunal de Justicia que responda a las cuestiones prejudiciales planteadas por el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia) del siguiente modo:

«El artículo 15, apartado 1, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea,

debe interpretarse en el sentido de que

no se opone a una normativa nacional que permite a los proveedores de servicios de comunicaciones electrónicas la conservación de los datos de identidad civil correspondientes a las direcciones IP y a una autoridad administrativa responsable de la protección de los derechos de autor y de los derechos afines frente a las violaciones de estos derechos cometidas en Internet el acceso limitado a tales datos con el fin de que dicha autoridad pueda identificar a los titulares de esas direcciones sospechosos de ser responsables de las referidas violaciones y pueda adoptar, en su caso, medidas contra ellos, sin que dicho acceso esté sujeto a un control previo por un órgano jurisdiccional o una entidad administrativa independiente, cuando dichos datos constituyen el único método de investigación para identificar a la persona que tenía atribuida esa dirección en el momento en que se cometió la infracción penal.»