Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
SR. MACIEJ SZPUNAR
presentadas el 28 de septiembre de 2023[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. A raíz de una solicitud de la Gran Sala, presentada con arreglo al artículo 60, apartado 3, del Reglamento de Procedimiento del Tribunal de Justicia, este decidió, el 7 de marzo de 2023, elevar el presente asunto al Pleno.

2. Mediante auto de 23 de marzo de 2023, el Tribunal de Justicia (Pleno) ordenó la reapertura de la fase oral del procedimiento e invitó a los interesados mencionados en el artículo 23 del Estatuto del Tribunal de Justicia de la Unión Europea, al Supervisor Europeo de Protección de Datos (SEPD) y a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) a participar en una nueva vista.

3. El 27 de octubre de 2022, presenté mis primeras conclusiones en este asunto antes de la terminación de la fase oral del procedimiento. Estas nuevas conclusiones me brindan por tanto la ocasión de profundizar en algunos puntos de mi razonamiento en este asunto respecto de los principales retos que plantean la conservación y el acceso a los datos personales.

[1] Lengua original: francés.

II. Marco jurídico

A. Derecho de la Unión

4. 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), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (DO 2009, L 337, p. 11) (en lo sucesivo, «Directiva 2002/58»).

[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. […]»

5. 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;

[…]».

6. 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.»

7. 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.»

8. 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.

[…]»

9. El artículo 15, apartado 1, de esta Directiva, 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 persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva [95/46]. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho [de la Unión], incluidos los mencionados en los apartados 1 y 2 del artículo 6 [TUE].»

B. Derecho francés

1. Código de la Propiedad Intelectual

10. 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; en lo sucesivo, «Hadopi»)] es una autoridad pública independiente.»

11. 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 […]».

12. 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.»

13. 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.»

14. 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)]. […]

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 n.º 2004 575 du 21 juin 2004 pour la confiance dans l'économie numérique [Ley n.º 2004 575, de 21 de junio de 2004, relativa a la confianza en la economía digital)].

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.»

15. 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;

– 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.»

16. 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.»

17. 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 […]»

18. 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 n.º 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 lo sucesivo, «Decreto de 5 de marzo de 2010»)] […] 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.

[…]»

19. 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;

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

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.»

20. 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

21. 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.

[…]»

22. 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.»

23. 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 Comunicaciones Electrónicas

24. El artículo L. 34-1 del Código de Correos y Comunicaciones Electrónicas, en su versión modificada por el artículo 17 de la loi n.º 2021-998 du 30 juillet 2021 [Ley n.º 2021-998 de 30 de julio de 2021], [5] dispone, en su apartado II *bis*:

«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.»

[5] JORF de 31 de julio de 2021, texto n.º 1. Esta versión del artículo L. 34-1 del Código, en vigor desde el 31 de julio de 2021, fue adoptada a raíz de la decisión del Conseil d'État (Consejo de Estado, Francia) 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 otro), el Conseil constitutionnel (Consejo Constitucional, Francia) declaró que esta versión anterior del artículo L. 34-1 del citado Código era contraria a la Constitución francesa 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, dicho 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).

III. Procedimiento ante el Tribunal de Justicia

25. En respuesta al requerimiento dirigido a los interesados mencionados en el artículo 23 del Estatuto del Tribunal de Justicia de la Unión Europea, los recurrentes en el litigio principal, los Gobiernos francés, danés, estonio, irlandés, neerlandés, finlandés y sueco, así como la Comisión Europea, respondieron a las preguntas escritas formuladas por el Tribunal de Justicia.

26. Estas mismas partes, con excepción del Gobierno finlandés, y los Gobiernos checo, español, chipriota, letón y noruego, el SEPD y la ENISA participaron en la vista celebrada el 15 de mayo de 2023.

IV. Análisis

27. Mi análisis de las cuestiones prejudiciales en mis primeras conclusiones me llevó a proponer al Tribunal de Justicia que declarase que el artículo 15, apartado 1, de la Directiva 2002/58 debe interpretarse en el sentido de que no se opone a una normativa nacional que permite la conservación, por parte de los proveedores de servicios de comunicaciones electrónicas, y el acceso, por parte de una autoridad administrativa como la Hadopi,[6] limitados 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 IP sospechosos de ser responsables de violaciones de los derechos de autor y de los derechos afines 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.

28. En las presentes conclusiones, trataré de profundizar en algunos elementos de mi anterior análisis y en las cuestiones debatidas en la vista celebrada el 15 de mayo de 2023, con el fin de exponer las razones por las que mantengo tanto mi propuesta de respuesta a las cuestiones prejudiciales como el razonamiento subyacente.[7]

29. Más concretamente, pondré de manifiesto que el hecho que se permita conservar y acceder a datos de identidad civil correspondientes a direcciones IP, sin control previo, con el fin de identificar a los infractores cuando tales datos constituyen el único método de identificación de estos últimos cumple los requisitos establecidos por el Tribunal de Justicia en relación con el examen de las medidas adoptadas con arreglo al artículo 15, apartado 1, de la Directiva 2002/58 (sección B).

6 El 1 de enero de 2022, el Conseil supérieur de l'audiovisuel (CSA) (Consejo Superior de lo Audiovisual) y la Hadopi pasaron a ser la Autorité de régulation de la communication audiovisuelle et numérique (Arcom) (Autoridad Reguladora de la Comunicación Audiovisual y Digital). No obstante, habida cuenta del período en el que se produjeron los hechos del litigio principal, en las presentes conclusiones me referiré a la Hadopi.

7 A este respecto, mantengo también mi propuesta de reformulación de las cuestiones prejudiciales y mi interpretación de su objeto. En efecto, aunque en las cuestiones prejudiciales, tal como están formuladas, únicamente se menciona el acceso a los datos de identidad civil correspondientes a direcciones IP, la cuestión del acceso a estos datos es indisociable de la de su conservación por los proveedores de servicios de comunicaciones electrónicas, de modo que el análisis de la compatibilidad de la conservación con el Derecho de la Unión es un requisito previo necesario para el examen de la compatibilidad del acceso. A este respecto, véanse los puntos 45 y siguientes de mis primeras conclusiones. Del mismo modo, aunque las cuestiones prejudiciales se refieren a «los datos de identidad civil correspondientes a una dirección IP», debe entenderse que también se refieren al acceso a las direcciones IP que permiten identificar el origen de una conexión. A este respecto, véanse los puntos 41 y siguientes de mis primeras conclusiones.

30. De este modo, demostraré que tal solución no supone un cambio de la jurisprudencia, exigente y protectora de los derechos fundamentales, desarrollada por el Tribunal de Justicia a raíz de las sentencias Tele2 Sverige y Watson y otros [8] y La Quadrature du Net y otros, [9] sino una evolución necesaria de esta jurisprudencia que, en mi opinión, está en consonancia con los principios consagrados por el Tribunal de Justicia. Esta distinción no es meramente semántica. En efecto, la solución que propongo no pretende poner en cuestión la jurisprudencia existente, sino permitir su adaptación, en pro de cierto pragmatismo, en circunstancias particulares y muy bien delimitadas (sección C).

31. En aras de la claridad y en la medida en que los debates mantenidos en la vista pusieron de manifiesto la necesidad de aportar precisiones a este respecto, comenzaré mi análisis recordando el funcionamiento del mecanismo de respuesta gradual de la Hadopi (sección A).

A. Mecanismo de respuesta gradual de la Hadopi

32. La Hadopi es una autoridad administrativa independiente 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 mecanismo denominado de «respuesta gradual», cuya aplicación incumbe a la Comisión de Protección de los Derechos de la Hadopi, se creó para cumplir esa misión.

33. La referida Comisión recibe denuncias presentadas por las organizaciones de titulares de derechos, de las que forman parte agentes jurados autorizados por el ministro de Cultura que recogen, en las redes *peer-to-peer*, las direcciones IP de los usuarios de Internet que ponen a disposición del público obras sin autorización de sus titulares. A continuación, se levantan actas en las que se indica, en particular, la dirección IP del acceso a Internet que se ha utilizado para cometer las violaciones de los derechos de autor, la fecha y hora de la violación constatada, así como el título de la obra en cuestión, y se transmiten a la Comisión de Protección de los Derechos de la Hadopi. A este respecto, procede subrayar, como ha señalado el SEPD, que el tratamiento de datos personales por parte de los agentes de los organismos de titulares de derechos está sujeto a la autorización de la Commission nationale de l'informatique et des libertés (CNIL) (Comisión Nacional de Informática y Libertades), autoridad francesa de control en materia de protección de datos. [10]

34. Una vez recibidas las actas, y tras un control automatizado para garantizar que contienen todos los datos requeridos, la Comisión de Protección de los Derechos de la Hadopi puede obtener de los proveedores de servicios de comunicaciones electrónicas la identidad, la dirección postal, la dirección de correo electrónico y los datos telefónicos del titular del abono que se haya utilizado para cometer una violación de los derechos de autor.

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

9 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).

10 Véase, a este respecto, la délibération n.º 2010-225 de la CNIL, du 10 juin 2010, modifiant l'autorisation de mise en œuvre par la Société des auteurs compositeurs et éditeurs de musique (SACEM) d'un traitement de données à caractère personnel ayant pour finalité la recherche et la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés «peer to peer» (autorisation n.º 1425421) [Acuerdo n.º 2010-225 de la CNIL, de 10 de junio de 2010, por el que se modifica la autorización a la Société des auteurs, compositeurs et éditeurs de musique (SACEM) (Sociedad de Autores, Compositores y Editores de Música) para que lleve a cabo un tratamiento de datos personales a los fines de la investigación y la comprobación de delitos de copia ilegal cometidos a través de redes de intercambio de archivos denominadas *peer-to-peer* (autorización n.º 1425421)].

35. A continuación, la Hadopi puede dirigir a dicho titular una «recomendación» en la que se le informe de que su acceso a Internet ha sido objeto de un uso contrario a los derechos de autor y se inste a la persona sospechosa de haber incumplido su obligación de vigilancia en cuanto al respeto en Internet de obras protegidas por los derechos de autor o los derechos afines a cumplir tal obligación. En otras palabras, la recomendación se dirige al titular del acceso a Internet, que en la práctica puede ser una persona distinta de la que ha puesto a disposición la obra en violación de los derechos de autor. Puede emitirse una segunda recomendación si vuelve a constatarse una violación cometida mediante el mismo punto de acceso a Internet. En caso de que vuelva a reincidirse, la Comisión de Protección de los Derechos de la Hadopi puede decidir poner el asunto en conocimiento del fiscal de la República para el ejercicio de acciones penales. A este respecto, como precisó el Gobierno francés en sus primeras observaciones, los agentes de la Hadopi encargados del mecanismo de respuesta gradual son agentes jurados autorizados por el presidente de la Hadopi, tienen un deber de secreto profesional y son los únicos, en el seno de la Hadopi, que están autorizados a acceder a los datos personales tratados en el contexto de dicho mecanismo.

36. Sobre este punto, debo precisar que los datos que se recogen y transmiten a la Hadopi no son los de la totalidad de los usuarios de las redes *peer-to-peer* que se limitan a descargar los contenidos,[11] sino únicamente los de las personas que han puesto a disposición contenidos ilegales, es decir, quienes los han *cargado*.

37. A título ilustrativo, en 2021, la Hadopi recibió casi cuatro millones de actas de las organizaciones de titulares de derechos, emitió 210 595 primeras recomendaciones y 53 564 segundas recomendaciones, y remitió 1 484 casos al fiscal de la República.

38. Una vez recordado lo anterior, expondré por qué opino que dicho mecanismo, que supone la conservación y el acceso a datos de identidad civil correspondientes a direcciones IP, es acorde con las exigencias de la jurisprudencia relativa a las medidas nacionales adoptadas con arreglo al artículo 15, apartado 1, de la Directiva 2002/58.

B. Cumplimiento de las exigencias derivadas de la jurisprudencia del Tribunal de Justicia relativa a la interpretación del artículo 15, apartado 1, de la Directiva 2002/58

39. Dado que, en mis primeras conclusiones, ya hice un repaso de la jurisprudencia del Tribunal de Justicia relativa a la conservación y al acceso a las direcciones IP atribuidas al origen de una conexión,[12] en las presentes conclusiones me centraré en lo que constituye, a mi parecer, el núcleo de dicha jurisprudencia, a saber, por un lado, la exigencia de proporcionalidad y, por el otro, en lo tocante al acceso a estos datos, la eventual necesidad de un control previo por un órgano jurisdiccional o una autoridad administrativa independiente.

1. Proporcionalidad de la medida en cuestión

40. Para determinar la compatibilidad con el Derecho de la Unión de una medida de conservación o de acceso a los datos de identidad civil correspondientes a una dirección IP, es preciso, como ha subrayado en reiteradas ocasiones el Tribunal de Justicia, proceder a una conciliación de los

[11] Sobre el funcionamiento de las redes *peer-to-peer* y los diferentes perfiles de internautas en dichas redes, véanse mis conclusiones presentadas en el asunto M.I.C.M. (C-597/19, EU:C:2020:1063), puntos 37 y siguientes.

[12] Puntos 53 y siguientes de mis primeras conclusiones.

distintos intereses legítimos y derechos en juego, a saber, por una parte, los derechos a la protección de la vida privada y a la protección de los datos personales,[13] garantizados por los artículos 7 y 8 de la Carta, y, por otra parte, la protección de los derechos y de las libertades de terceros consagrados en los artículos 3, 4, 6 y 7 de la Carta.[14] He de añadir que, en el presente asunto, los derechos a la protección de la vida privada y a la protección de datos personales también deben conciliarse con el derecho de propiedad reconocido en el artículo 17 de la Carta, en la medida en que el mecanismo de respuesta gradual está destinado en última instancia a proteger los derechos de autor y los derechos afines.

41. El Tribunal de Justicia ha precisado, a este respecto, que la conciliación que debe llevarse a cabo en virtud del artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros adoptar una medida que suponga una excepción al principio de confidencialidad cuando tal medida sea «*necesaria, proporcionada y apropiada* en una sociedad democrática» (el subrayado es mío). El considerando 11 de esta Directiva precisa que este tipo de medidas deben ser «rigurosamente» *proporcionales* al fin que se pretende alcanzar.[15]

42. Por otra parte, el Tribunal de Justicia se refiere al principio de proporcionalidad en todo su razonamiento relativo a la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 y lo convierte así en la piedra angular del examen de cualquier medida nacional de conservación o de acceso a los datos personales adoptada en virtud de dicha disposición.

43. De una lectura más detenida de este razonamiento se desprende que el principio de proporcionalidad incluye, en el contexto del artículo 15, apartado 1, de la Directiva 2002/58, distintas partes, relativas, por un lado, a la gravedad de la injerencia en los derechos fundamentales que implica la conservación o el acceso a los datos de tráfico y, por el otro, a la necesidad de la medida en cuestión.

44. En cuanto a la conservación y el acceso por la Hadopi a los datos de identidad civil correspondientes a direcciones IP, considero que tanto la gravedad de la injerencia como el carácter indispensable de estos datos deberían llevar al Tribunal de Justicia a modular su examen de la proporcionalidad de una medida nacional adoptada con arreglo al artículo 15, apartado 1, de la Directiva 2002/58.

a) Gravedad relativa de la injerencia en los derechos fundamentales

45. De reiterada jurisprudencia del Tribunal de Justicia se desprende claramente que, conforme al principio de proporcionalidad, la importancia del objetivo perseguido por una medida adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58 debe ser correlativa a la gravedad de la injerencia que supone la medida.[16]

[13] Los derechos a la protección de la vida privada y a la protección de los datos personales se traducen, en el contexto de la Directiva 2002/58, en los principios de confidencialidad de las comunicaciones y de prohibición del almacenamiento de los datos de dichas comunicaciones que en ella se recogen.

[14] Sentencias La Quadrature du Net y otros, apartados 120 a 122, 127 y 128; 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), apartados 48 y 50, y de 20 de septiembre de 2022, SpaceNet y Telekom Deutschland (C-793/19 y C-794/19, en lo sucesivo, «sentencia SpaceNet y Telekom Deutschland», EU:C:2022:702), apartados 63 y 65.

[15] Sentencias La Quadrature du Net y otros, apartado 129, Commissioner of An Garda Síochána y otros, apartado 51, y SpaceNet y Telekom Deutschland, apartado 66.

[16] Sentencias Commissioner of An Garda Síochána y otros, apartado 56, y SpaceNet y Telekom Deutschland, apartado 71.

46. Más concretamente, el Tribunal de Justicia ha declarado, como expuse en mis primeras conclusiones, 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». [17]

47. Por lo que respecta a las direcciones IP, el Tribunal de Justicia ha observado que, si bien presentan un grado de sensibilidad menor que los demás datos de tráfico, su conservación y análisis sí constituyen una injerencia grave en los derechos fundamentales, puesto que pueden utilizarse para llevar a cabo el rastreo exhaustivo de la secuencia de navegación de un internauta y, en consecuencia, para establecer el perfil detallado de este y extraer conclusiones precisas sobre su vida privada. [18]

48. En el litigio principal, la conservación y el acceso a los datos de identidad civil correspondientes a direcciones IP persiguen luchar contra las violaciones de los derechos de autor y de los derechos afines a los derechos de autor. Pues bien, en mi opinión, es evidente que esa lucha no puede considerarse comprendida en la lucha contra la delincuencia grave, [19] aun cuando el volumen de tales violaciones tenga un carácter masivo. Existe, pues, un desfase entre la gravedad de la injerencia en los derechos fundamentales que implica la medida en cuestión y el objetivo que persigue.

49. En mis primeras conclusiones, consideré, de conformidad con la jurisprudencia del Tribunal de Justicia, que el acceso de la Hadopi a los datos de identidad civil correspondientes a una dirección IP constituye ciertamente una injerencia grave en los derechos fundamentales. Aunque también señalé que debían permitirse la conservación y el acceso a dichos datos, tras la vista debo realizar algunas precisiones.

50. El mecanismo de respuesta gradual permite a la Hadopi vincular la dirección IP comunicada por las organizaciones de titulares de derechos de personas sospechosas de haber utilizado su acceso a Internet para cometer una violación de los derechos de autor en una red *peer-to-peer* a la identidad civil de esta persona, así como un extracto del archivo cargado en violación de los derechos de autor. Como señalaron la Comisión y el SEPD en la vista, tales elementos, pese a que sin duda permiten obtener más información que la mera identidad del presunto autor de una infracción penal, no llevan a extraer conclusiones muy precisas sobre la vida privada de esa persona. En efecto, como indiqué en mis primeras conclusiones, [20] se trata únicamente de revelar una consulta puntual de un contenido que, considerado de forma aislada, no permite establecer el perfil detallado de la persona que la hizo.

[17] Sentencias Tele2, apartado 115; de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), apartado 56, y de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, en lo sucesivo, «sentencia Prokuratuur», EU:C:2021:152), apartado 33. Véase también el punto 92 de mis primeras conclusiones.

[18] Véanse las sentencias La Quadrature du Net y otros, apartados 152 y 153; Commissioner of An Garda Síochána y otros, apartado 73, y SpaceNet et Telekom Deutschland, apartado 103. Véanse también los puntos 63, 64 y 93 de mis primeras conclusiones.

[19] En mis primeras conclusiones, afirmé que, al objeto de evitar que los Estados miembros eludan los requisitos del artículo 15, apartado 1, de la Directiva 2002/58, el concepto de «delincuencia grave» debe recibir una interpretación autónoma. Me reafirmo en esta postura. No obstante, he de subrayar que, aun cuando el Tribunal de Justicia declarase que incumbe a los Estados miembros definir el concepto de «delincuencia grave», este debería establecerse en todo caso dentro de los límites del Derecho de la Unión y no podría ampliarse hasta el punto de vaciar de contenido dicha disposición.

[20] Punto 101 de mis primeras conclusiones.

51. Ello es tanto más cierto cuanto que, para empezar, la gran mayoría de las direcciones IP comunicadas a la Hadopi constituyen direcciones IP «dinámicas», que son, por naturaleza, cambiantes y solo corresponden a una identidad precisa en un único momento, que coincide con la puesta a disposición del contenido de que se trate. Excluyen, por tanto, cualquier rastreo exhaustivo.

52. A continuación, debo precisar que no me parece que la protección de los derechos fundamentales en Internet pueda justificar que no se permita acceder únicamente a los datos relativos a la dirección IP, al contenido de una obra y a la identidad de la persona que la ha puesto a disposición vulnerando los derechos de autor; antes bien, entiendo que bastaría con establecer ciertas garantías en cuanto a la conservación y el acceso a dichos datos. La siguiente analogía con una situación real me parece pertinente: una persona sospechosa de haber cometido un robo no puede invocar su derecho a la protección de la vida privada para que las personas responsables de perseguir este delito no puedan tener conocimiento del contenido robado. En cambio, esa persona puede, con razón, invocar sus derechos fundamentales para impedir que durante el procedimiento se acceda a un conjunto de datos más amplio que los exclusivamente necesarios para calificar el presunto delito.

53. Por último, he de observar que, contrariamente a lo que alegan los recurrentes, el mecanismo de respuesta gradual no parece implicar una supervisión generalizada de los usuarios de las redes *peer-to-peer*. En efecto, no se trata de comprobar toda su actividad en una red determinada al objeto de dilucidar si han llevado a cabo una puesta a disposición de una obra vulnerando los derechos de autor, sino más bien de determinar, a partir de un archivo identificado como ilegal, el titular del acceso a Internet desde el que el internauta ha procedido a la puesta a disposición. Del mismo modo, como subrayó el SEPD en la vista, tampoco se trata de supervisar la actividad de todos los usuarios de las redes *peer-to-peer*, sino únicamente la de las personas que cargan los archivos ilegales, en el entendido de que la carga de estos archivos es tanto menos reveladora de información sobre la vida privada de la persona cuanto que puede llevarse a cabo con el solo propósito de que los internautas puedan proceder a renglón seguido a descargar otros archivos.

54. En estas circunstancias, las razones que llevaron al Tribunal de Justicia a considerar que la conservación y el acceso a las direcciones IP constituyen una injerencia grave en los derechos fundamentales no me parecen aplicables a un mecanismo de respuesta gradual como el de la Hadopi. De ello se deduce que la gravedad de la injerencia que suponen esa conservación y ese acceso debe matizarse en el examen del principio de proporcionalidad.

55. En otras palabras, considero que la jurisprudencia del Tribunal de Justicia relativa a la gravedad de la injerencia en los derechos fundamentales resultante de la conservación y el acceso a direcciones IP debe interpretarse en el sentido de que no implica que tal injerencia sea grave en todo caso, sino que únicamente lo es cuando las direcciones IP puedan conducir a un rastreo exhaustivo de la secuencia de navegación del internauta y a extraer conclusiones muy precisas sobre su vida privada.

56. Dado que no es eso lo que sucede en una situación como la examinada en el litigio principal, la injerencia que suponen la conservación y el acceso a los datos de identidad civil correspondientes a una dirección IP utilizada para poner a disposición un contenido vulnerando los derechos de autor debería poder justificarse por un objetivo de lucha contra la delincuencia que no se limite exclusivamente a la delincuencia grave.

57. Debo precisar, además, que la injerencia en los derechos fundamentales que suponen la conservación y el acceso a datos de identidad civil correspondientes a una dirección IP en una situación como la examinada en el litigio principal no reviste mayor gravedad porque el titular del acceso a Internet utilizado para la puesta a disposición de un contenido ilegal no sea necesariamente el responsable de esta puesta a disposición, de modo que la recomendación dirigida por la Hadopi podría llevar a revelar a dicho titular dicho contenido al que un tercero haya podido acceder. Por una parte, he de recordar que la infracción penal objeto de indagación por la Hadopi es el incumplimiento de la obligación de velar por que el acceso no sea objeto de una utilización con fines de puesta a disposición de un contenido en violación de los derechos de autor. Por tanto, es necesario que la información que permita su calificación se transmita a su presunto autor. Por otra parte, como ya he señalado, considero que la información relativa a la obra en cuestión no permite extraer conclusiones precisas sobre la vida privada de la persona que llevó a cabo la puesta a disposición. Por consiguiente, la posible transmisión de esta información al titular de la conexión a Internet no va más allá de lo necesario para permitir la persecución de la violación de los derechos de autor en cuestión.

b) Carácter indispensable de los datos en cuestión para el descubrimiento y la persecución de una infracción penal

58. Para garantizar la proporcionalidad de una medida de conservación y de acceso a datos de tráfico como los datos de identidad civil correspondientes a una dirección IP adoptada con arreglo al artículo 15, apartado 1, de la Directiva 2002/58, es preciso, según la jurisprudencia del Tribunal de Justicia, que la injerencia que suponga se limite al mínimo estrictamente necesario para que pueda alcanzarse el objetivo perseguido.[21] A mi juicio, esto es precisamente lo que sucede con la medida en cuestión en el litigio principal.

59. Como expuse en mis primeras conclusiones,[22] de la propia jurisprudencia del Tribunal de Justicia resulta que, en el caso de una infracción penal cometida exclusivamente en línea, como la vulneración de los derechos de autor en una red *peer-to-peer*, la dirección IP puede constituir el único método de investigación para identificar a la persona que tenía atribuida esa dirección en el momento en que se cometió.[23] De ello se deduce, en mi opinión, que la conservación y el acceso a los datos de identidad civil correspondientes a direcciones IP con el objetivo de descubrir y perseguir las violaciones de los derechos de autor cometidas en línea son, con arreglo a la jurisprudencia, estrictamente necesarios para alcanzar el objetivo perseguido.

60. Es cierto que toda exigencia de protección de los datos personales supone una limitación de las facultades de investigación. Ello resulta del propio principio de conciliación de intereses contrapuestos y tal resultado no puede, como tal, discutirse. Ahora bien, en el supuesto de que la dirección IP constituya el único método para identificar a la persona sospechosa de haber cometido una violación en línea de un derecho de propiedad intelectual, tal situación difiere de la mayor parte de acciones penales, sobre las que el Tribunal de Justicia ha afirmado que su «eficacia […] depende generalmente no de un solo medio de investigación, sino de todos los medios de investigación que se hallen a disposición de las autoridades nacionales competentes a los referidos efectos».[24] Admitir que los datos de identidad civil correspondientes a direcciones IP no deban ser

[21] Sentencias La Quadrature du Net y otros, apartados 120 a 122, y 132; Commissioner of An Garda Síochána y otros, apartados 48 y 54, y SpaceNet y Telekom Deutschland, apartados 63 y 69.

[22] Punto 78 de mis primeras conclusiones.

[23] Sentencias La Quadrature du Net y otros, apartado 154, Commissioner of An Garda Síochána y otros, apartado 73, y SpaceNet y Telekom Deutschland, apartado 100.

[24] Sentencia Commissioner of An Garda Síochána y otros, apartado 69.

objeto de conservación y de acceso en una situación como la concurrente en el litigio principal no da lugar, como cualquier otra medida que garantice la protección de los datos de tráfico, a una mera limitación de las facultades de investigación, sino que priva a las autoridades nacionales del único método de descubrimiento y persecución de determinadas infracciones penales.

61. Dicho de otro modo, según la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 que propongo, no se trata de permitir, mediante el examen de la necesidad de tal medida, la conservación y el acceso a datos que meramente *faciliten* el descubrimiento y la persecución de infracciones penales, cuando también puedan ser descubiertas y perseguidas por otros medios concurrentes, incluso menos eficaces. Antes bien, se trata de permitir la conservación y el acceso a esos datos cuando sea *indispensable* para identificar a la persona sospechosa de haber cometido una infracción penal que no podría ser perseguida sin esos medios, por constituir los datos en cuestión el único instrumento de identificación del internauta en la medida en que se comete exclusivamente en línea.

62. Tal interpretación se impone, en mi opinión, a menos que se acepte que toda una serie de infracciones penales no puedan ser nunca perseguidas. [25]

63. A mi parecer, de todo lo anterior se desprende que una normativa nacional que permite la conservación, por parte de los proveedores de servicios de comunicaciones electrónicas, y el acceso, por parte de una autoridad administrativa, limitados a los datos de identidad civil correspondientes a direcciones IP es plenamente proporcionada al objetivo pretendido, a saber, la persecución de violaciones de los derechos de autor y de los derechos afines a los derechos de autor en Internet, en la medida en que la injerencia en los derechos fundamentales que suponen es de una gravedad limitada y en que tales datos constituyen el único método de investigación que permite identificar a la persona que tenía atribuida dicha dirección en el momento de la comisión de la infracción penal.

64. Por consiguiente, considero que el artículo 15, apartado 1, de la Directiva 2002/58 debe interpretarse en el sentido de que no se opone a dicha normativa.

2. Existencia de garantías materiales y procedimentales adecuadas

65. Por lo que respecta específicamente al acceso a datos de identidad civil correspondientes a direcciones IP, de la jurisprudencia del Tribunal de Justicia se desprende que la proporcionalidad estricta de la medida no basta para que resulte compatible con el artículo 15, apartado 1, de la Directiva 2002/58.

66. En efecto, para garantizar que el acceso a datos de tráfico y de localización se limite a lo estrictamente necesario, el Tribunal de Justicia ha declarado que es esencial que dicho acceso se supedite a un control previo efectuado, bien por un órgano jurisdiccional, bien por un órgano administrativo independiente que disponga de todas las atribuciones y presente todas las garantías necesarias para conciliar los diferentes intereses legítimos y derechos de que se trate. [26]

[25] Punto 81 de mis primeras conclusiones. Véanse también, a este respecto, los puntos 79 y siguientes de las presentes conclusiones.

[26] Sentencias Tele2, apartado 120; Prokuratuur, apartados 51 y 52, y Commissioner of An Garda Síochána y otros, apartados 106 y 107.

67. Una interpretación estricta de la jurisprudencia llevaría, por tanto, a considerar que el acceso por la Hadopi a los datos de identidad civil correspondientes a las direcciones IP de las personas sospechosas de haber cometido una violación de los derechos de autor en Internet debería estar sujeto a dicho control previo, que no está previsto en el mecanismo de respuesta gradual en su configuración actual.

68. Sin embargo, como alegó el Gobierno irlandés en la vista y como expuse en mis primeras conclusiones, considero que el requisito del control previo por un órgano jurisdiccional o por una entidad administrativa independiente no es una exigencia sistemática, sino que depende de un análisis más global de la medida en cuestión que tenga en cuenta tanto la gravedad de la injerencia que supone como las garantías que prevé.

69. En efecto, debo señalar que, en todas y cada una de las sentencias que enunciaron esta exigencia de control previo por un órgano jurisdiccional o por una entidad administrativa independiente, se cuestionaban normativas nacionales que permitían acceder a todos los datos de tráfico y de localización de los usuarios relativos a todos los medios de comunicaciones electrónicas de usuarios [27] o, cuando menos, a la telefonía fija y móvil [28] de usuarios identificados.

70. De ello deduzco que la exigencia de tal control previo debe estar guiada por la gravedad de la injerencia de que se trate en los asuntos en cuestión. Como declaró el Tribunal de Justicia, eran datos que «efectivamente puede[n] permitir extraer conclusiones precisas —incluso muy precisas — sobre la vida privada de las personas […], como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan». [29] Además, se trataba de los datos de personas ya identificadas y sospechosas de haber cometido una infracción penal sobre la base de otros indicios, de manera que los datos de que se trataba permitían reforzar los elementos de cargo contra el usuario en cuestión ampliando el alcance de los datos que lo concernían.

71. Pues bien, en cuanto atañe a la normativa controvertida en el litigio principal, y como he señalado, la gravedad de la injerencia que supone vincular un dato de identidad civil y una dirección IP es mucho menor que la resultante de acceder a todos los datos de tráfico y de localización de una persona, en la medida en que esa vinculación no aporta ningún elemento que permita extraer conclusiones precisas sobre la vida privada de la persona afectada.

72. Por otra parte, como indiqué en mis primeras conclusiones, [30] estos datos solo se refieren a las personas que, a raíz de una constatación objetiva de un uso de la dirección IP contrario a un derecho de autor determinada por las organizaciones de titulares de derechos, han cometido hechos que pueden constituir un incumplimiento de la obligación de vigilancia prevista en el artículo L. 336-3 del CPI. No han sido previamente identificadas por otros medios, puesto que la vinculación de la dirección IP a los datos de identidad civil es el único método para la identificación de la persona en cuestión. Por tanto, el acceso a estos datos no permite, como sucedía en los asuntos sobre los que el Tribunal de Justicia se ha pronunciado, obtener información adicional y precisa sobre la actividad de personas que ya son sospechosas sobre la

27 Sentencias Tele2 y Commissioner of An Garda Síochána y otros.

28 Sentencia Prokuratuur.

29 Sentencia Prokuratuur, apartado 36.

30 Punto 102 de mis primeras conclusiones.

base de otros elementos, sino únicamente permitir la explotación de la dirección IP, que por lo demás carece de interés. En estas circunstancias, los datos a los que tiene acceso la Hadopi son de hecho limitados.

73. En mi opinión, existe una diferencia fundamental entre acceder a datos personales relativos a una persona sospechosa de haber cometido una infracción penal para demostrar su culpabilidad y permitir desvelar la identidad del autor de una infracción penal ya constatada.

74. Ello es tanto más cierto cuanto que, tal como yo lo entiendo, para recabar direcciones IP en las redes *peer-to-peer* se necesita una autorización previa limitada únicamente a estos datos, de modo que la Hadopi en ningún caso dispone de un conjunto ilimitado de datos respecto de los internautas sospechosos de haber cometido una violación de los derechos de autor en Internet. [31]

75. Por tanto, la lógica que subyace al requisito del control previo efectuado por un órgano jurisdiccional o una entidad administrativa independiente no se aplica en cuanto atañe a un mecanismo de respuesta gradual como el que es objeto del litigio principal, de modo que dicho requisito no me parece necesario para garantizar que la injerencia en los derechos fundamentales que supone ese mecanismo se limite a lo estrictamente necesario.

76. De todo lo anterior resulta que una normativa nacional que permite la conservación y el acceso, por una autoridad administrativa independiente como la Hadopi, a datos de identidad civil correspondientes a direcciones IP con el fin de identificar a los titulares de esas direcciones sospechosos de haber violado los derechos de autor, sin que dicho acceso esté supeditado a un control previo por un órgano jurisdiccional o una entidad administrativa independiente, es acorde, en definitiva, con los principios establecidos por la jurisprudencia del Tribunal de Justicia, cuando tales datos constituyen el único método de identificación de la persona que tenía atribuida la dirección IP en el momento de la comisión de la infracción penal, de modo que el artículo 15, apartado 1, de la Directiva 2002/58 debe interpretarse en el sentido de que no se opone a tal normativa.

77. Más allá de estas consideraciones propias del asunto objeto del litigio principal, debo formular ciertas observaciones más generales sobre la necesidad de esta evolución de la jurisprudencia del Tribunal de Justicia.

C. Evolución de la jurisprudencia necesaria y limitada

78. Son varios los argumentos a favor de que se precise la jurisprudencia del Tribunal de Justicia relativa a la conservación y el acceso a datos como las direcciones IP correspondientes a los datos de identidad civil.

79. En primer lugar, como ya he subrayado, [32] en la situación examinada en el litigio principal, la obtención de los datos de identidad civil correspondientes a una dirección IP es el único método de investigación que permite identificar a la persona que tenía atribuida dicha dirección en el momento en que se cometió la infracción penal.

[31] Punto 33 de las presentes conclusiones.

[32] Punto 59 de las presentes conclusiones.

80. De ello resulta necesariamente que, si el Tribunal de Justicia considerase, no obstante, que el artículo 15, apartado 1, de la Directiva 2002/58 se opone a la conservación y el acceso a tales datos, las autoridades nacionales se verían privadas de hecho de este único método de identificación y, por tanto, los autores de la infracción penal en cuestión nunca podrían ser perseguidos. [33] Esto me llevó, en mis primeras conclusiones, a evocar el riesgo de impunidad sistémica para esta infracción penal. [34]

81. El riesgo de impunidad sistémica no se limita a las violaciones de los derechos de autor cometidas en las redes *peer-to-peer*, sino que se extiende, como alegó el Gobierno checo en la vista, a todas las infracciones penales cometidas exclusivamente en línea.

82. En efecto, las infracciones penales cuyo autor solo puede ser identificado a través de su dirección IP nunca podrían perseguirse y las disposiciones que las castigan nunca podrían aplicarse si se considerase que tanto la conservación de los datos como el acceso a ellos son contrarios al Derecho de la Unión.

83. A este respecto, debo añadir que, como han alegado los recurrentes en el litigio principal, es cierto que, en teoría, los autores de determinadas infracciones penales cometidas exclusivamente en línea podrían identificarse a través de otros métodos. En este sentido, se refieren, en particular, al identificador utilizado en las redes sociales y a los datos vinculados a la cuenta del usuario, su dirección de correo electrónico, su número de teléfono o información sobre su vida privada que la persona haya revelado. Sin embargo, para vincular tales datos a la identidad de la persona, deben llevarse a cabo investigaciones exhaustivas durante las cuales se examine la actividad en línea del internauta. Por tanto, considero que, a diferencia de la dirección IP, utilizar tales métodos de investigación puede posibilitar que se extraigan conclusiones muy precisas sobre la vida privada de las personas, de modo que la conservación y el acceso a esos datos serían, en este sentido, contrarios al artículo 15, apartado 1, de la Directiva 2002/58.

84. En estas circunstancias, es cierto que el acceso a los datos de identidad civil correspondientes a la dirección IP de un internauta no es, desde el punto de vista teórico, el único método de investigación que permite identificar al titular de esa dirección en el momento en que se cometió la infracción penal, pero sí es el que permite perseguirlo con la menor injerencia en sus derechos fundamentales y, por tanto, evitar la impunidad general.

85. En segundo lugar, he de insistir en que tal solución permitiría, a mi parecer, conciliar dos líneas de jurisprudencia del Tribunal de Justicia, fuentes de una cierta tensión a la que me referí en mis primeras conclusiones [35] y en las presentadas en el asunto M.I.C.M., [36] a saber, por un lado, la jurisprudencia sobre la conservación y el acceso a los datos y, por el otro, la relativa a la comunicación de las direcciones IP atribuidas al origen de una conexión en el marco de los recursos para la protección de los derechos de propiedad intelectual interpuestos por personas privadas.

86. En tercer lugar, si bien es cierto que la jurisprudencia del Tribunal de Justicia a partir de las sentencias Tele2 y La Quadrature du Net y otros merece aplauso en la medida en que ha permitido establecer un marco de protección de los derechos fundamentales de los usuarios de servicios de comunicaciones electrónicas, no deja de estar marcada por una cierta casuística. En

[33] Punto 62 de las presentes conclusiones.

[34] Puntos 78 y siguientes de mis primeras conclusiones.

[35] Puntos 69 y siguientes de mis primeras conclusiones.

[36] C-597/19, EU:C:2020:1063.

efecto, en los asuntos sometidos a su examen, el Tribunal de Justicia ha venido precisando progresivamente su jurisprudencia y ha tenido la ocasión de examinar distintas normativas nacionales a la luz del artículo 15, apartado 1, de la Directiva 2002/58. Sin embargo, el Tribunal de Justicia no puede presagiar virtualmente todas las medidas que podrían ser objeto de análisis a la luz de esta disposición. Prueba de ello es el número de peticiones de decisión prejudicial [37] que se han planteado ante él desde la sentencia Tele2, lo que demuestra, en mi opinión, la dificultad que pueden experimentar los órganos jurisdiccionales nacionales al aplicar los principios dimanantes de la jurisprudencia del Tribunal de Justicia a situaciones distintas de las que dieron lugar a las sentencias en cuestión. [38]

87. De ello se sigue, por tanto, en mi opinión, que es necesario un cierto grado de flexibilidad cuando se someten al examen del Tribunal de Justicia medidas que no podían contemplarse en sentencias anteriores, como las normativas relativas a infracciones penales que solo pueden perseguirse en la medida en que los datos de identidad civil correspondientes a direcciones IP sean conservados y accesibles, de las que el Tribunal de Justicia no había conocido hasta la fecha.

88. Así pues, no se trata, como sostuvo el Gobierno danés, de reconsiderar la jurisprudencia del Tribunal de Justicia, sino de admitir que, sobre la base de los principios que la sustentan, pueda llegarse a una solución más matizada, en circunstancias muy limitadas.

89. En efecto, la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 que propongo solo permite conservar y acceder a datos de identidad civil correspondientes a direcciones IP al objeto de la persecución de infracciones penales cuyos autores, a falta de tales datos, no podrían ser identificados. Por consiguiente, tal interpretación se refiere únicamente a las infracciones penales cometidas exclusivamente en Internet y no pone en cuestión las soluciones que figuran en la jurisprudencia en materia de conservación y acceso a datos más amplios y que persiguen otros objetivos.

V. Conclusión

90. Habida cuenta del conjunto de consideraciones anteriores, propongo al Tribunal de Justicia que responda a las cuestiones prejudiciales planteadas por el Conseil d'Etat (Consejo de Estado, 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

[37] Sentencias de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); La Quadrature du Net y otros; Prokuratuur, Commissioner of An Garda Síochána y otros y SpaceNet y Telekom Deutschland.

[38] A este respecto, el creciente número de peticiones de decisión prejudicial que tienen por objeto la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 también puede indicar cierta suerte de reticencia por parte de los órganos jurisdiccionales nacionales a aplicar los principios establecidos por el Tribunal de Justicia a situaciones ligeramente diferentes, debido a las particularidades de los ordenamientos jurídicos nacionales. Sobre este punto, véanse, en particular, Cameron, I.: «Metadata retention and national security: *Privacy international* and *La Quadrature du Net*», *Common Market Law Review*, 2021, vol. 58, n.º 5, pp. 1433 a 1471, o Bertrand, B.: «L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin?», *Dalloz IP/IT*, 2021, n.º 9, pp. 468 a 472. Por consiguiente, me parece esencial, con la perspectiva de mantener un diálogo fructífero entre el Tribunal de Justicia y los órganos jurisdiccionales de los Estados miembros, que el Tribunal de Justicia pueda dar muestras de adaptación cuando las circunstancias así lo exijan. Como se ha señalado en la doctrina, el nivel elevado de protección garantizado por la jurisprudencia del Tribunal de Justicia no puede ser realmente eficaz sin la adhesión de los órganos jurisdiccionales nacionales, principales responsables de su aplicación. Sobre este punto, véanse, en particular, Teyssedre, J.: «Strictly regulated retention and access regimes for metadata: *Commissioner of An Garda Siochana*», *Common Market Law Review*, vol. 60, n.º 2, 2023, pp. 569 a 588, y Sirinelli, J.: «La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite», *Revue trimestrielle de droit européen*, vol. 57, n.º 2, 2021, pp. 313 a 329.

comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea,

debe interpretarse en el sentido de que

no se opone a una normativa nacional que permite la conservación, por parte de los proveedores de servicios de comunicaciones electrónicas, y el acceso, por parte de 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, limitados 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, cuando dichos datos constituyen el único método de investigación para identificar a las personas que tenían atribuidas esas direcciones en el momento en que se cometió la infracción penal.»