

[Salta la navegación del artículo para ir al principio.](#)

Consejo de Estado

n.º 433539

ECLI:FR:CECHR:2026:433539.20260430

No publicado en la colección Lebon

Cámaras 10 y 9 combinadas

el Sr. Stéphane Eustache, ponente;

FITZJEAN O COBHTHAIGH, abogados;

Lectura del jueves 30 de abril de 2026

REPÚBLICA FRANCESA

EN NOMBRE DEL PUEBLO FRANCÉS

Teniendo en cuenta el siguiente procedimiento:

Mediante decisión interlocutoria de 5 de julio de 2021, el Consejo de Estado, actuando en su calidad de juez, en primer lugar, desestimó las alegaciones del Ministro de Cultura que solicitaban que se registrara la retirada automática de las asociaciones La Quadrature du Net, French Data Network, Franciliens.net y Fédération des fournisseurs d'accès à internet associatifs (Federación de Asociaciones de Proveedores de Internet); en segundo lugar, desestimó los argumentos basados en la falta de fundamentación, la falta de base jurídica, la violación del Reglamento (UE) 2016/679, de 27 de abril de 2016, y el derecho a un recurso efectivo, dirigidos contra la decisión tácita por la que el Primer Ministro rechazó la solicitud de estas asociaciones para derogar el Decreto n.º 2010-236, de 5 de marzo de 2010; Finalmente, aplazó su decisión sobre las alegaciones que solicitaban la anulación por abuso de poder de esta decisión implícita, a la espera de una resolución del Tribunal de Justicia de la Unión Europea. El Tribunal Europeo de Derechos Humanos se pronunció sobre las siguientes cuestiones preliminares:

- 1) ¿Se incluyen los datos de identidad civil correspondientes a una dirección IP entre los datos de tráfico o de localización que, en principio, están sujetos a la obligación de control previo por parte de un tribunal o un órgano administrativo independiente con potestad vinculante?
- 2) Si la respuesta a la primera pregunta es afirmativa, y teniendo en cuenta la baja sensibilidad de los datos relativos a la identidad civil de los usuarios, incluidos sus datos de contacto, ¿debe interpretarse la

Directiva de 12 de julio de 2002 relativa al tratamiento de datos personales y a la protección de la privacidad en el sector de las comunicaciones electrónicas, interpretada a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, en el sentido de que impide que la legislación nacional prevea la recogida de dichos datos correspondientes a las direcciones IP de los usuarios por parte de una autoridad administrativa, sin el control previo de un tribunal o un órgano administrativo independiente con potestad vinculante?

3) Si la respuesta a la segunda pregunta es sí, y dada la baja sensibilidad de los datos de identidad civil, el hecho de que solo se puedan recoger dichos datos, únicamente con el fin de prevenir incumplimientos de obligaciones definidas de manera precisa, exhaustiva y restrictiva por la legislación nacional, y el hecho de que el control sistemático del acceso a los datos de cada usuario por parte de un tribunal o una entidad administrativa de terceros con poderes vinculantes pudiera comprometer el desempeño de la misión de servicio público encomendada a la autoridad administrativa independiente que realiza esta recogida de datos, ¿impide la directiva que dicho control se lleve a cabo utilizando métodos apropiados, como el control automatizado, cuando proceda bajo la supervisión de un servicio interno dentro del organismo que ofrezca garantías de independencia e imparcialidad con respecto a los agentes responsables de llevar a cabo esta recogida de datos?

En una sentencia de 30 de abril de 2024 (C-470/21), el Tribunal de Justicia de la Unión Europea respondió a las cuestiones prejudiciales del Consejo de Estado.

Teniendo en cuenta los demás documentos del expediente;

Teniendo en cuenta:

- la Carta de los Derechos Fundamentales de la Unión Europea;
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016;
- Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001;
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002;
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016;
- Código Penal;
- Código de Comunicaciones Postales y Electrónicas;
- Código de Propiedad Intelectual;
- Código de Relaciones entre el Público y la Administración;
- Ley n.º 86-1067, de 30 de septiembre de 1986;

- Decreto n.º 2010-236, de 5 de marzo de 2010;
- Sentencia del Tribunal de Justicia de la Unión Europea, de 30 de abril de 2024 (C-470/21);
- el Código de Justicia Administrativa;

Después de escuchar en audiencia pública:

- el informe del Sr. Stéphane Eustache, Maestro de Solicitudes,
- las alegaciones de la Sra. Charline Nicolas, Relatora Pública;

Considerando lo siguiente:

1. Las asociaciones La Quadrature du Net, French Data Network, Franciliens.net y Fédération des fournisseurs d'accès à internet associatifs (Federación de Proveedores de Servicios de Internet Comunitarios) solicitaron al Consejo de Estado la anulación, por abuso de poder, de la decisión implícita por la que el Primer Ministro rechazó su petición de derogación del decreto de 5 de marzo de 2010, relativo al tratamiento automatizado de datos personales autorizado por el artículo L. 331-23 del Código de la Propiedad Intelectual, conocido como el «Sistema de medidas de gestión para la protección de las obras en Internet». Mediante decisión interlocutoria de 5 de julio de 2021, el Consejo de Estado, actuando en su calidad de juez, suspendió su decisión sobre estas alegaciones hasta que el Tribunal de Justicia de la Unión Europea se pronunciara sobre las cuestiones prejudiciales que le había planteado. Mediante sentencia C-470/21, de 30 de abril de 2024, el Tribunal de Justicia de la Unión Europea respondió a estas cuestiones.

Sobre el marco jurídico de la Unión Europea:

2. De conformidad con el artículo 2 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la privacidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y comunicaciones electrónicas), «datos de tráfico» significa «todos los datos tratados con el fin de enrutar una comunicación a través de una red de comunicaciones electrónicas o para su facturación» y «datos de localización» significa «todos los datos tratados en una red de comunicaciones electrónicas que indican la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible públicamente». Según el apartado 1 del artículo 5 de la presente Directiva: «Los Estados miembros garantizarán, mediante legislación nacional, la confidencialidad de las comunicaciones realizadas

a través de una red pública de comunicaciones y de servicios de comunicaciones electrónicas de acceso público, así como la confidencialidad de los datos de tráfico relacionados. En particular, prohibirán a cualquier persona distinta de los usuarios escuchar, interceptar, almacenar las comunicaciones y los datos de tráfico relacionados, o someterlos a cualquier otro medio de interceptación o vigilancia, sin el consentimiento de los usuarios afectados, salvo que dicha persona esté legalmente autorizada a ello de conformidad con el artículo 15, apartado 1. Lo dispuesto en este apartado no impedirá el almacenamiento técnico necesario para la transmisión de una comunicación, sin perjuicio del principio de confidencialidad». Según el artículo 6 de esta Directiva: «1. Los datos de tráfico relativos a los abonados y usuarios tratados y almacenados por el prestador de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible públicamente deben suprimirse o anonimizarse cuando ya no sean necesarios para la transmisión de una comunicación, sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el artículo 15, apartado 1. / 2. Los datos de tráfico necesarios para la elaboración de las facturas de los abonados y los pagos de interconexión podrán ser tratados. Dicho tratamiento solo está permitido hasta el final del plazo durante el cual la factura pueda ser impugnada legalmente o puedan iniciarse procedimientos judiciales para obtener el pago. / 3. Con el fin de comercializar sus servicios de comunicaciones electrónicas o prestar servicios de valor añadido, El proveedor de un servicio de comunicaciones electrónicas de acceso público podrá tratar los datos a que se refiere el párrafo 1 en la medida y durante el tiempo necesarios para la prestación o comercialización de dichos servicios, siempre que el suscriptor o usuario afectado por esos datos haya dado su consentimiento (...).

3. De conformidad con el apartado 1 del artículo 15 de la misma Directiva: «Los Estados miembros podrán adoptar medidas legislativas destinadas a limitar el alcance de los derechos y obligaciones previstos en los artículos 5 y 6, el artículo 8, apartados 1, 2, 3 y 4, y el artículo 9 de la presente Directiva, cuando dicha limitación sea una medida necesaria, adecuada y proporcionada en una sociedad democrática para salvaguardar la seguridad nacional —es decir, la seguridad del Estado—, la defensa y la seguridad pública, o para garantizar la prevención, la investigación, la detección y el enjuiciamiento de delitos o del uso no autorizado del sistema de comunicaciones electrónicas, según lo dispuesto en el artículo 13, apartado 1, de la Directiva 95/46/CE. A tal efecto, los Estados miembros podrán, entre otras cosas, adoptar medidas legislativas que prevean la conservación de datos durante un período limitado cuando ello esté justificado por alguno de los motivos enumerados en el presente apartado. Todas las medidas a que se refiere el presente apartado se adoptarán de conformidad con los principios

generales del Derecho comunitario, incluidos los a que se refieren los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea.»

En lo que respecta a la retención de datos personales por parte de los proveedores de servicios de comunicaciones electrónicas:

4. De las disposiciones citadas en los puntos 2 y 3, tal como las interpretó el Tribunal de Justicia de la Unión Europea en su sentencia de 30 de abril de 2024, se desprende que un Estado miembro puede exigir a los proveedores de servicios de comunicaciones electrónicas, en virtud del apartado 1 del artículo 15 de la Directiva de 12 de julio de 2002, que garanticen la retención general e indiscriminada de las direcciones IP de sus usuarios a efectos de la lucha contra los delitos penales en general, cuando se excluya efectivamente que dicha retención pueda dar lugar a una injerencia grave en la vida privada de las personas afectadas debido a la posibilidad de extraer conclusiones precisas sobre ellas mediante, en particular, la vinculación de esas direcciones IP con un conjunto de datos de tráfico o de localización que también habrían sido retenidos por los proveedores.

5. Para evitar tales injerencias, corresponde al Estado miembro establecer en su legislación normas claras y precisas que garanticen una separación hermética de los datos en poder de los proveedores de servicios de comunicaciones electrónicas. Estas normas deben exigir que cada categoría de datos, incluidos los relativos a la identidad civil y las direcciones IP, se mantenga completamente separada de las demás categorías de datos; que esta separación hermética se garantice eficazmente mediante un sistema informático seguro y fiable; que la vinculación de las direcciones IP con la identidad civil del interesado se realice mediante un proceso técnico de alto rendimiento que no comprometa la eficacia de la separación hermética de estas categorías de datos; y, por último, que la fiabilidad de este almacenamiento sea objeto de una supervisión periódica por parte de una autoridad pública distinta de la que solicita el acceso a los datos en poder de los proveedores de servicios de comunicaciones electrónicas.

En cuanto al acceso de una autoridad pública nacional a datos de identidad civil:

6. Las disposiciones citadas en los puntos 2 y 3, según la interpretación de la sentencia de 30 de abril de 2024 del Tribunal de Justicia de la Unión Europea, no impiden que una autoridad pública nacional, responsable de la protección de los derechos de autor y derechos conexos frente a las infracciones de estos derechos cometidas en Internet, acceda, a efectos de la lucha contra los delitos en general, a los datos de identidad civil de los abonados a servicios de comunicaciones

electrónicas, correspondientes a direcciones IP, con el único fin de identificar a las personas sospechosas de haber cometido dichas infracciones y, en su caso, adoptar medidas contra ellas. Sin embargo, puesto que la misma autoridad pública puede vincular estos datos de identidad, de forma reiterada para la misma persona, con información, incluso limitada, relativa al contenido de obras puestas ilegalmente a disposición en Internet, y así obtener información sobre aspectos, incluso sensibles, de la vida privada de las personas afectadas, dicho acceso debe estar regulado por la legislación nacional.

7. A este respecto, en primer lugar, el Tribunal de Justicia de la Unión Europea dictamina que los agentes con acceso a dicha información deben tener prohibido, por un lado, divulgar, en cualquier forma, información sobre el contenido de los archivos consultados por las personas interesadas, salvo únicamente con el fin de remitir el asunto al Ministerio Público, y por otro lado, rastrear la actividad de navegación de estas personas y, en general, utilizar sus direcciones IP para fines distintos de identificar a sus titulares con vistas a adoptar posibles medidas contra ellos.

8. En segundo lugar, el Tribunal de Justicia de la Unión Europea dictamina que, cuando una autoridad pública ya ha vinculado dos veces los datos de identidad de una misma persona con información relativa al contenido de obras publicadas ilegalmente en Internet, no puede vincularlos una tercera vez sin haber sido autorizada para ello por un tribunal o un organismo administrativo independiente. Por consiguiente, el Tribunal considera, como se desprende claramente de los fundamentos y la parte dispositiva de la sentencia, que dicha revisión, que no puede automatizarse por completo, debe realizarse previamente, salvo en casos de urgencia debidamente justificados, por un organismo con plenos poderes y que ofrezca todas las garantías necesarias para asegurar un equilibrio entre los diversos intereses y derechos legítimos en juego. Cuando la realice una entidad administrativa, esta deberá tener la capacidad de actuar con objetividad e imparcialidad, y deberá ser un tercero independiente de la autoridad que solicita el acceso a los datos.

9. Además, de los fundamentos de la sentencia del Tribunal de Justicia de la Unión Europea de 30 de abril de 2024 se desprende que, cuando se sospeche que la persona en cuestión ha cometido actos que constituyen delitos penales en general, el tribunal o el organismo administrativo independiente responsable de realizar la verificación a que se refiere el punto anterior deberá denegar el acceso a los datos relativos a la identidad civil cuando dicho acceso permita a la autoridad pública solicitante extraer conclusiones específicas sobre la vida privada de esa persona. Por el contrario, dicho acceso podrá autorizarse cuando la información puesta en conocimiento de ese tribunal u organismo

administrativo independiente genere sospechas de que la persona en cuestión ha cometido actos que constituyen delitos graves.

10. En tercer lugar, el Tribunal de Justicia de la Unión Europea ha dictaminado que el tratamiento de datos personales utilizado por una autoridad pública debe someterse, a intervalos regulares, a auditorías realizadas por un organismo independiente, que actúe como tercero en relación con dicha autoridad pública, con el fin de verificar la integridad del sistema, incluidas las salvaguardias efectivas contra los riesgos de uso indebido o acceso y uso ilícitos de los datos, así como su eficacia y fiabilidad en la detección de cualquier infracción.

En cuanto al marco jurídico nacional:

11. De conformidad con el artículo L. 336-3 del Código de la Propiedad Intelectual, el titular del acceso a los servicios de comunicación pública en línea tiene la obligación de garantizar que dicho acceso no se utilice para la reproducción, ejecución, puesta a disposición o comunicación al público de obras u objetos protegidos por derechos de autor o derechos conexos sin la autorización de los titulares de los derechos, cuando dicha autorización sea necesaria. Para garantizar el cumplimiento de esta obligación, la Autoridad Reguladora de las Comunicaciones Audiovisuales y Digitales (ARCOM), actuando a solicitud de los órganos de defensa profesional debidamente constituidos, los órganos de gestión colectiva, el Centro Nacional de Cine e Imágenes de Animación, o sobre la base de la información transmitida por el Ministerio Público o un informe del alguacil elaborado a solicitud del titular de los derechos, es responsable de aplicar las medidas de protección para las obras y objetos a los que se adjunta un derecho de autor o un derecho conexo, según lo definido en los artículos L. 331-19 a L. 331-24 del mismo código, que se rigen por el denominado procedimiento de "respuesta gradual".

12. De conformidad con el artículo L. 331-13 y el párrafo I del artículo L. 331-14 del Código de la Propiedad Intelectual, esta misión es llevada a cabo por el miembro de ARCOM designado de conformidad con el párrafo IV del artículo 4 de la Ley de 30 de septiembre de 1986 sobre libertad de comunicación, así como por funcionarios públicos juramentados ante la autoridad judicial y autorizados por el Presidente de ARCOM en las condiciones establecidas en los artículos R. 331-2 a R. 331-5 del mismo Código. De conformidad con el artículo 8 de esta Ley, este miembro y estos funcionarios están obligados al secreto profesional respecto de los hechos, acciones e información que hayan podido conocer en el ejercicio de sus funciones, bajo las condiciones y sanciones previstas en los artículos 413-9 y 413-10 del Código Penal.

13. Como se establece en el primer párrafo del artículo L. 331-20 del Código de la Propiedad Intelectual, el procedimiento de respuesta gradual consiste en enviar a los suscriptores que hayan cometido actos susceptibles de constituir una infracción de la obligación definida en el artículo L. 336-3 del mismo Código una recomendación que les recuerde el contenido de dicha obligación, les inste a cumplirla y les advierta de las sanciones que se acarrearán. Si tales actos se repiten en un plazo de seis meses, el segundo párrafo del mismo artículo L. 331-20 dispone que la autoridad podrá enviar una nueva recomendación con la misma información que la anterior, pero acompañada de una carta certificada o cualquier otro medio que permita acreditar la fecha de presentación de esta recomendación. Si, en el plazo de un año a partir de esta segunda recomendación, se observan nuevas infracciones, el artículo R. 331-12 del mismo Código dispone que la autoridad informará al interesado, mediante carta certificada, de que dichos actos son susceptibles de enjuiciamiento. Cuando corresponda, de conformidad con el artículo R. 331-14 del mismo código, la decisión del miembro competente de ARCOM, que determine que los hechos son susceptibles de constituir el delito de negligencia grave definido en el artículo R. 335-5 o los delitos de infracción previstos en los artículos L. 335-2, L. 335-3 y L. 335-4 del mismo código, se transmite al fiscal público del tribunal judicial competente.

14. Para los efectos de esta respuesta gradual, el artículo L. 331-23 del Código de la Propiedad Intelectual autoriza a ARCOM a implementar el procesamiento automatizado de datos personales bajo las condiciones definidas por un decreto del Consejo de Estado, emitido después de consulta con la Comisión Nacional de Informática y Libertades Civiles. Como se prevé en el párrafo I del artículo 4 y el anexo del decreto impugnado de 5 de marzo de 2010 relativo al tratamiento automatizado de datos personales autorizado por el artículo L. 331-23 del Código de la Propiedad Intelectual, conocido como el "Sistema para la gestión de medidas de protección de las obras en Internet", los miembros y agentes competentes de ARCOM tienen "acceso directo", por un lado, a los datos personales transmitidos por las personas y autoridades que han remitido el asunto a ARCOM y que se refieren en particular a la "dirección IP" de la persona que cometió los actos denunciados, la "información relativa a las obras u objetos protegidos afectados por los actos" y el "nombre del archivo tal como se encuentra en el ordenador del abonado" y, por otro lado, a los datos personales obtenidos de los operadores de comunicaciones electrónicas, en particular los "apellidos, nombre" del abonado, su "dirección postal y direcciones de correo electrónico", su "número de teléfono" y la "dirección de la instalación telefónica".

En cuanto a la legalidad de la impugnada negativa a revocar:

15. De conformidad con el artículo L. 243-2 del Código de Relaciones entre el Público y la Administración: «La administración está obligada a derogar expresamente un acto reglamentario ilegal u obsoleto, ya sea que esta situación existiera desde su promulgación o resulte de circunstancias legales o fácticas posteriores, a menos que la ilegalidad haya cesado». El efecto práctico de la anulación por abuso de poder de la negativa a derogar un acto reglamentario ilegal radica en la obligación, que el juez puede ordenar de oficio según lo dispuesto en el artículo L. 911-1 del Código de Justicia Administrativa, de que la autoridad competente derogue dicho acto para cesar las infracciones ilícitas que su vigencia continua causa al ordenamiento jurídico. En consecuencia, cuando se le presenta una solicitud de anulación de la negativa a derogar un acto reglamentario, el juez que revisa la actuación administrativa está obligado a evaluar la legalidad del acto reglamentario cuya derogación se solicita a la luz de las normas aplicables en la fecha de su decisión.

16. En primer lugar, si bien el Ministro de Cultura sostiene que los cuatro principales proveedores de servicios de Internet que operan en Francia conservan datos relativos a la identidad civil de los abonados y su "tráfico IP" en condiciones que cumplen con los requisitos establecidos en el punto 5, ninguna disposición legal exige dicha conservación, en esas condiciones, a los operadores de comunicaciones electrónicas, en lo que respecta a la lucha contra los delitos en general. En consecuencia, los demandantes tienen razón al argumentar que el decreto de 5 de marzo de 2010 es ilícito en la medida en que no limita los datos registrados en el tratamiento a aquellos que han sido conservados por los operadores de comunicaciones electrónicas en condiciones que cumplen con los requisitos del Derecho de la Unión Europea, tal como se describe en el punto 5. Por lo tanto, tienen razón al argumentar que la negativa a derogar el decreto de 5 de marzo de 2010 es, en ese sentido, ilícita.

17. En segundo lugar, si bien es cierto que el miembro y los agentes competentes de ARCOM aplican, de conformidad con lo dispuesto en el punto 12, el procedimiento de respuesta gradual en cumplimiento de los requisitos de confidencialidad y protección de la privacidad establecidos en el punto 7, ninguna disposición exige que estas personas soliciten autorización judicial o administrativa independiente, en las condiciones previstas en el punto 8, para acceder a los datos de identidad de una persona que, aun habiendo sido objeto de dos recomendaciones de conformidad con el artículo L. 331-20 del Código de la Propiedad Intelectual, ha cometido por tercera vez actos que puedan constituir una infracción de la obligación prevista en el artículo L. 336-3 del mismo Código. Sin embargo, como ha dictaminado el Tribunal de Justicia de la Unión Europea, dicho acceso en esta fase del procedimiento de respuesta gradual puede revelar información potencialmente sensible relativa a aspectos de la vida privada del interesado y, por lo tanto, debe

ser autorizado previamente por un tribunal o por un órgano administrativo independiente de ARCOM, que actúe de forma objetiva e imparcial.

18. En consecuencia, los solicitantes tienen razón al argumentar que las disposiciones del artículo 4, apartado 1, del Decreto de 5 de marzo de 2010, en la medida en que autorizan al miembro de ARCOM y a los agentes mencionados en el punto 12 a acceder, por tercera vez para la misma persona, a los datos de identidad almacenados en el sistema de tratamiento sin que dicho acceso esté sujeto a la autorización de un tribunal o un órgano administrativo independiente, infringen los requisitos derivados del Derecho de la Unión Europea. Por lo tanto, están justificados al argumentar que la negativa a derogar el Decreto de 5 de marzo de 2010 es, en ese sentido, ilícita.

19. De todo lo anterior se desprende que la decisión impugnada debe ser anulada en la medida en que se niega a anular el decreto impugnado únicamente porque, en primer lugar, a efectos de combatir los delitos penales en general, no limita los datos registrados en el tratamiento que establece a aquellos datos que han sido retenidos por operadores de comunicaciones electrónicas en condiciones que cumplen los requisitos, recordados en el punto 5, del Derecho de la Unión Europea, y porque, en segundo lugar, las disposiciones del párrafo I de su artículo 4 autorizan al miembro y a los agentes de ARCOM mencionados en el punto 12 a acceder directamente a los datos de identidad de una persona que, aun habiendo sido objeto de dos recomendaciones de conformidad con el artículo L. 331-20 del Código de la Propiedad Intelectual, Cometido por tercera vez actos susceptibles de constituir un incumplimiento de la obligación estipulada en el artículo L. 336-3 del mismo código.

Respecto a los efectos de la anulación pronunciada:

20. En primer lugar, si bien el Ministro de Cultura argumenta que la promulgación e implementación de las disposiciones necesarias para el pleno cumplimiento de los requisitos europeos ignorados por el decreto de 5 de marzo de 2010 requiere un retraso de doce meses en los efectos de la anulación, el expediente no demuestra que la anulación inmediata de la negativa a derogar las disposiciones impugnadas responda a una necesidad imperiosa que justifique, de manera excepcional, una excepción al principio de que un tribunal nacional no puede modular los efectos de una anulación judicial resultante de una infracción del Derecho de la Unión Europea. Por consiguiente, deben rechazarse los argumentos del Ministro de Cultura que pretenden modular los efectos de la anulación a lo largo del tiempo.

21. En segundo lugar, la anulación de la decisión del Primer Ministro de

negarse a derogar el decreto de 5 de marzo de 2010 implica únicamente que se le ordene derogar dicho decreto en la medida en que sus disposiciones contravengan los requisitos derivados del Derecho de la Unión Europea, sin necesidad de imponer una multa por incumplimiento.

22. En tercer lugar, la anulación pronunciada por esta decisión implica necesariamente que ARCOM debe abstenerse de aplicar las disposiciones legislativas que, por las razones expuestas anteriormente, contravienen los requisitos derivados del Derecho de la Unión Europea. Para garantizar la continuidad de su misión de combatir el delito de negligencia grave, que contribuye en particular a los objetivos establecidos por la Directiva europea de 22 de mayo de 2001 sobre la armonización de determinados aspectos de los derechos de autor y derechos conexos en la sociedad de la información, ARCOM podrá, en espera de la promulgación de las disposiciones necesarias para cumplir con los requisitos mencionados en el punto 5, seguir solicitando a los operadores de comunicaciones electrónicas el acceso a los datos personales de los abonados cuyas direcciones IP le hayan sido transmitidas por los responsables de garantizar la protección de los derechos de autor y derechos conexos, solo si se establece que dichos operadores han almacenado estos datos en las condiciones establecidas en el punto 5. Sin embargo, dado que estas condiciones de almacenamiento no son necesarias para la consecución de un objetivo que se enmarque dentro del ámbito de los delitos graves, ARCOM podrá, sin necesidad de verificar su aplicación, solicitar dicho acceso a los operadores de comunicaciones electrónicas cuando los hechos que se le presenten sean susceptibles de constituir los delitos definidos en los artículos L. 335-2, L. 335-3 o L. 335-4 del Código de la Propiedad Intelectual y se enmarquen dentro del ámbito de los delitos graves. delito grave.

23. Finalmente, la anulación pronunciada por esta decisión no impide que el miembro y los agentes de ARCOM mencionados en el punto 12 accedan a los datos de identidad de una persona, mientras se promulgan las disposiciones necesarias para cumplir con los requisitos mencionados en el punto 8, únicamente con el propósito de enviarles la primera o la segunda de las dos recomendaciones sucesivas previstas en el artículo L. 331-20 del Código de la Propiedad Intelectual.

24. En las circunstancias del presente caso, se ordenará al Estado que pague a las asociaciones La Quadrature du Net, French Data Network, Franciliens.net y Fédération des fournisseurs d'accès à internet associatifs la suma de 1.000 € cada una, de conformidad con el artículo L. 761-1 del Código de Justicia Administrativa.

DECIDE:

Artículo 1: Se anula la decisión del Primer Ministro en lo que respecta a la derogación de las disposiciones del Decreto n.º 2010-236, de 5 de marzo de 2010, que, por las razones expuestas en la presente decisión, no cumplen con los requisitos del Derecho de la Unión Europea.

Artículo 2: Se ordena al Primer Ministro que derogue las disposiciones del Decreto de 5 de marzo de 2010, en la medida prevista en el artículo 1.

Artículo 3: La anulación pronunciada en el artículo 1 implica para ARCOM las obligaciones definidas en los fundamentos de la presente decisión.

Artículo 4: El Estado abonará a las asociaciones La Quadrature du Net, French Data Network, Franciliens.net y Fédération des fournisseurs d'accès à internet associatifs la suma de 1000 € cada una, de conformidad con el artículo L. 761-1 del Código de Justicia Administrativa.

Artículo 5: Se desestima el resto de la solicitud.

Artículo 6: Esta decisión se notificará a la asociación La Quadrature du Net, mencionada en primer lugar, al Primer Ministro, al Ministro de Cultura, a la Autoridad Reguladora de la Comunicación Audiovisual y Digital y a la Comisión Nacional de Informática y Libertades.