Asunto C-140/20

Resumen de la petición de decisión prejudicial con arreglo al artículo 98, apartado 1, del Reglamento de Procedimiento del Tribunal de Justicia

Fecha de presentación:

25 de marzo de 2020

Órgano jurisdiccional remitente:

Supreme Court (Tribunal Supremo, Irlanda)

Fecha de la resolución de remisión:

25 de marzo de 2020

Parte demandante:

G. D.

Parte demandada:

Commissioner of the Garda Síochána (Comisario del cuerpo de la policía nacional)

Minister for Communications, Energy and Natural Resources (Ministro de Comunicaciones, Energía y Recursos Naturales)

Attorney General (Fiscal General)

Objeto del procedimiento principal

El presente procedimiento se refiere al régimen jurídico vigente en Irlanda en virtud de la Communications (Retention of Data) Act 2011 [Ley sobre comunicaciones (conservación de datos) de 2011], que regula la conservación y el acceso a los metadatos de las telecomunicaciones por las autoridades nacionales de Irlanda y en particular por el cuerpo de la policía nacional irlandesa («An Garda Síochána») en la detección, investigación y enjuiciamiento de delitos graves.

DOCUMENTO DE TRABAJO

Objeto y fundamento jurídico de la petición de decisión prejudicial

Determinar si la Ley de comunicaciones (conservación de datos) de 2011, y en particular su artículo 6, apartado 1, es contraria al artículo 15, apartado 1, de la Directiva 2002/58/CE.

Cuestiones prejudiciales

«1) ¿Un régimen general o universal de conservación de datos, aunque esté sujeto a restricciones rigurosas tanto por lo que se refiere a la conservación como al acceso de los datos, es por sí mismo contrario a las disposiciones del artículo 15 de la Directiva 2002/58/CE, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea?

2) A la hora de decidir si es contraria al Derecho de la Unión una medida nacional, aplicada sobre la base de la Directiva 2006/24/CE, que establece un régimen general de conservación de datos sujeto a los necesarios controles estrictos en materia de conservación y de acceso a los mismos, y en particular a la hora de valorar la proporcionalidad de dicho régimen, ¿es lícito que un órgano jurisdiccional nacional tenga en cuenta el hecho de que los proveedores del servicio pueden legalmente conservar los datos para sus propios fines comerciales y se les puede exigir que conserven esos datos por razones de seguridad nacional excluidas de las disposiciones de la Directiva 2002/58/CE?

3) ¿Qué criterios debería aplicar un órgano jurisdiccional nacional, en el examen de la compatibilidad con el Derecho de la Unión Europea y, en particular, con la Carta de los Derechos Fundamentales de la Unión Europea, de una medida nacional relativa al acceso a los datos conservados, para determinar si tal régimen de acceso contempla el control previo independiente exigido según la jurisprudencia del Tribunal de Justicia? En dicho contexto ¿puede un órgano jurisdiccional nacional, al hacer tal valoración, tener en cuenta la existencia de un control judicial o independiente posterior?

4) En cualquier caso, ¿está un órgano jurisdiccional nacional obligado a declarar una medida nacional contraria a las disposiciones del artículo 15 de la Directiva 2002/58/CE si dicha medida establece un régimen general de conservación de datos a los fines de la lucha contra los delitos graves y el órgano jurisdiccional nacional ha llegado a la conclusión, de acuerdo con todas las pruebas disponibles, de que tal conservación de datos es esencial y estrictamente necesaria para alcanzar los fines de la lucha contra los delitos graves?

5) ¿Si un órgano jurisdiccional nacional está obligado a concluir que una medida nacional es contraria a las disposiciones del artículo 15 de la Directiva 2002/58/CE, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, puede lícitamente limitar el efecto temporal de dicha declaración si entiende que, de no hacerlo, se causaría un «desorden y perjuicio para el interés general» [en línea, por ejemplo, con el enfoque adoptado en el asunto R *(National*

DOCUMENTO DE TRABAJO

Council for Civil Liberties) contra Secretary of State for Home Department y Secretary of State for Foreign Affairs [2018] EWHC 975, apartado 46]?

6) ¿Está autorizado un órgano jurisdiccional nacional al que se le pide que declare que la legislación nacional es contraria al artículo 15 de la Directiva 2002/58/CE o que no aplique dicha legislación o que declare que su aplicación ha vulnerado los derechos de una persona, en el contexto de un procedimiento iniciado para defender una posición respecto de la admisibilidad de las pruebas en un proceso penal o en cualquier otra circunstancia, a denegar tal pretensión en lo que se refiere a los datos conservados con arreglo a una disposición nacional aprobada en virtud de la obligación que impone el artículo 288 TFUE de incorporar fielmente a la legislación nacional las disposiciones de una directiva, o a limitar tal declaración al período posterior a la sentencia del TJUE de 8 de abril de 2014 por la que se declara la invalidez de la Directiva 2006/24/CE?»

Disposiciones del Derecho de la Unión invocadas

Tratado de la Unión Europea, artículos 5, apartado 4 y 6, apartado 1 y Protocolo n.º 21.

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

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31)

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 2002, L 201, p. 37)

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO 2006, L 105, p. 54)

Sentencia de 10 de febrero de 2009, Irlanda/Parlamento Europeo y Consejo de la Unión Europea (C-301/06, EU:C:2009:68)

Sentencia de 26 de noviembre de 2009, Comisión/Irlanda (C-202/09, EU:C:2009:736)

Sentencia de 8 de abril de 2014, Digital Rights Ireland Limited/Minister for Communications, Marine and Natural Resources y otros y Kärntner

DOCUMENTO DE TRABAJO

Landesregierung y otros (asuntos acumulados C-293/12 y C-594/12, EU:C:2014:238)

Sentencia de 21 de diciembre de 2016, Tele2 Sverige AB/Post— och telestyrelsen y Secretary of State for the Home Department/Tom Watson y otros (asuntos acumulados C-203/15 y C-698/15, EU:C:2016:970)

Disposiciones de Derecho nacional invocadas

Communications (Retention of Data) Act 2011 [Ley de comunicaciones (conservación de datos) de 2011] (en lo sucesivo, «Ley de 2011»).

La Ley de 2011 fue aprobada con la finalidad expresa de incorporar la Directiva de 2006. El artículo 3 de dicha Ley exige a todos los proveedores de servicios que conserven «los datos de la telefonía de red fija y móvil» durante un período de dos años. Estos datos identifican la fuente, el destino, la fecha y hora del comienzo y de la terminación de la comunicación, el tipo de comunicación de que se trata, así como el tipo de los equipos utilizados y su ubicación geográfica. El contenido de las comunicaciones no entra en esta categoría de datos.

Mediante una solicitud de transmisión se puede tener acceso a los datos conservados y estos pueden ser transmitidos. El artículo 6 de la Ley de 2011 establece las condiciones con arreglo a las cuales se puede presentar una solicitud de transmisión de datos, y, según su apartado 1, los miembros del An Garda Síochána que no tengan un rango inferior a comisario jefe podrán presentar una solicitud de transmisión de datos si consideran que estos son necesarios para, entre otros fines, prevenir, detectar, investigar o enjuiciar un delito grave. Se define como «delito grave» aquel que es punible como mínimo con pena de prisión de cinco años, así como los demás delitos que figuran en el Anexo 1 de la Ley.

Entre los mecanismos de control previstos en la Ley de 2011 se incluyen el procedimiento de denuncia regulado en su artículo 10 y las obligaciones del artículo 12 relativas al «juez designado», al que le corresponde la función de revisar la aplicación de las disposiciones contenidas en dicha Ley.

Por razones de política interna, el jefe del An Garda Síochána, el Garda Commissioner, determinó que las solicitudes de transmisión de datos de telefonía que se presentasen con arreglo a la Ley de 2011 debían tramitarse de forma centralizada por un único comisario jefe. El detective comisario jefe al que se encomendó la responsabilidad de la transmisión de datos era el jefe del departamento de inteligencia y seguridad del An Garda Síochána, a quien corresponde en última instancia decidir si se presenta una solicitud de transmisión de datos a los proveedores de servicios de comunicaciones con arreglo a las disposiciones de la Ley de 2011. Se creó una pequeña unidad independiente, denominada Telecommunications Liaison Unit (en lo sucesivo, «TLU») con el fin de dar apoyo al detective comisario jefe en sus tareas y de actuar como único punto de contacto con los proveedores del servicio.

DOCUMENTO DE TRABAJO

En la época pertinente para la presente investigación, todas las solicitudes de transmisión de datos tenían que ser aprobadas en primera instancia por un comisario (o un inspector que actuase en calidad de comisario) para ser posteriormente enviadas a la TLU para su tramitación. Se ordenó a los investigadores que incluyeran la información suficiente en las solicitudes para que se pudiera tomar una decisión bien informada y se les dijo que tuvieran en cuenta que el comisario jefe podría tener que justificar posteriormente dicha decisión ante un órgano jurisdiccional o ante el juez designado de la High Court (Tribunal Superior, Irlanda). Tanto a la TLU como al detective comisario jefe se les exige que comprueben la legalidad, proporcionalidad y necesidad de las solicitudes de transmisión de datos que presentan los miembros del An Garda Síochána. Aquellas solicitudes que se considerase que no cumplían los requisitos previstos en la ley o en los protocolos internos de la policía irlandesa eran devueltas para que se hicieran las correspondientes aclaraciones o se aportara más información. De acuerdo con lo previsto en un Memorando de Acuerdo de mayo de 2011, los operadores del servicio no tramitarían solicitudes de datos relacionados con llamadas que no pasaran por dicho proceso. La TLU está sujeta además a auditoría obligatoria por el Data Protection Commissioner (Comisario para la protección de datos).

Breve exposición de los hechos y del procedimiento principal

1 En marzo de 2015, el jurado declaró al demandante («G. D.») culpable del asesinato de la Sra. O'H., por lo que se le impuso la pena de cadena perpetua. El condenado negó su culpabilidad en todo momento. Dicha condena fue recurrida por G. D. ante la Irish Court of Appeal (Tribunal de Apelación, Irlanda), estando pendiente aún el proceso. En el transcurso de este, G. D. impugnó sin éxito la admisibilidad de ciertas pruebas presentadas por la acusación que se basaban en datos de telefonía conservados.

2 Paralelamente, G. D inició el presente procedimiento civil para cuestionar determinadas disposiciones de la Ley de 2011 al amparo de las cuales se conservaron los referidos metadatos de telefonía y se pudo acceder a los mismos. El demandante pretende que se declare la invalidez de la correspondiente disposición legal, con el fin de poder sostener en el recurso interpuesto contra su sentencia condenatoria que las pruebas obtenidas con los datos de telefonía no deberían haber sido admitidas en aquel proceso y, por tanto, su condena había sido temeraria. Los demandados (en lo sucesivo, el «Estado») solicitan que se confirme la validez de las disposiciones legales.

3 Mediante resolución de 6 de diciembre de 2018 en el asunto Dwyer/Commissioner of An Garda Síochána y otros [2018] IEHC 685, la High Court (Tribunal Superior) estimó la solicitud de G. D. para que el artículo 6, apartado 1, párrafo a) de la Ley de 2011 fuera declarado contrario al artículo 15, apartado 1, de la Directiva 2002/58/CE, en relación con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea.

DOCUMENTO DE TRABAJO

4 El Estado presentó recurso contra dicha resolución ante el Supreme Court (Tribunal Supremo), que ahora plantea la presente petición de decisión prejudicial.

5 El Supreme Court (Tribunal Supremo) declara ser consciente de que unas pruebas como las presentadas en el proceso penal seguido contra G. D. cada vez tienen mayor peso a la hora de detectar y enjuiciar determinadas categorías de delitos graves. A juzgar por la experiencia del Supreme Court (Tribunal Supremo), algunos asuntos similares solo se pudieron resolver gracias a la disponibilidad del tipo de datos a los que se refiere el presente procedimiento.

6 El Supreme Court (Tribunal Supremo) afirma que dichos asuntos a menudo tenían que ver con delitos graves contra mujeres, niños y otras personas vulnerables y que no sería posible detectar o enjuiciar a su autor sin tal clase de pruebas. En efecto, el Supreme Court (Tribunal Supremo) indica que, como en el asunto de G. D., los servicios de telefonía se utilizan con el fin de acosar sexualmente o de aprovecharse de otro modo de las personas vulnerables.

7 El Supreme Court (Tribunal Supremo) hace hincapié en que no es posible tener acceso a lo que no se ha conservado. Si no se permitiese la conservación de metadatos con carácter universal, aun con las dificultades de acceso que se pudieran establecer, muchos de esos delitos graves no se podrían llegar a detectar ni a enjuiciar satisfactoriamente.

8 El Supreme Court (Tribunal Supremo) efectúa las siguientes consideraciones fácticas:

1) otras formas alternativas de conservación de datos, mediante la georreferenciación u otros medios, no serían eficaces para alcanzar los objetivos de prevención, investigación, detección y enjuiciamiento de, al menos, determinados tipos de delitos graves, además de que posiblemente se violaran otros derechos de la persona;

2) un objetivo de conservación de datos por otros métodos menos severos que un régimen general de conservación sujeto a las necesarias garantías resulta inviable, y

3) los objetivos de prevención, investigación, detección y enjuiciamiento de delitos graves se verían seriamente comprometidos en ausencia de un régimen general de conservación de datos.

Alegaciones esenciales de las partes en el procedimiento principal

9 El demandante alega que el artículo 6, apartado 1, letra a) de la Ley de 2011, en virtud del cual se conservaron los metadatos y se tuvo acceso a ellos, que fueron admitidos como prueba en el procedimiento penal seguido contra él, es inválido por su incompatibilidad con el artículo 15, apartado 1, de la Directiva 2002/58.

DOCUMENTO DE TRABAJO

10 El demandante sostiene que la conservación universal de datos es inadmisible, con independencia de las garantías existentes en cuanto al acceso a los mismos. Alega asimismo que el régimen de acceso no prevé la suficiente protección independiente contra el acceso inapropiado a los datos. El demandante sostiene que las garantías contempladas en la Ley de 2011 son mínimas y que esta no establece unas normas claras y precisas que indiquen bajo qué circunstancias y en qué condiciones los proveedores de servicio deben facilitar el acceso a los datos a las autoridades nacionales, tal y como exige el TJUE. En particular, considera que el sistema existente de autocertificación de las solicitudes de transmisión de datos aplicado por el An Garda Síochána no satisface el requisito de que las solicitudes de acceso estén sujetas a una revisión previa por parte de un órgano jurisdiccional o bien por un organismo administrativo independiente, como se declara en el apartado 120 de la sentencia en el asunto *Tele2 Sverige*.

11 Los demandados (el «Estado») sostienen que la ley es válida. Alegan que es preciso partir de un examen global para determinar si el régimen legal en cuestión protege los derechos de privacidad de una forma proporcionada.

12 Los demandados consideran que la Ley de 2011 establecía un marco detallado que regulaba el acceso a los datos conservados. Además, el Estado alega que la TLU, que ejerce sus funciones de forma independiente con respecto al An Garda Síochána, cumple el requisito de ser un «organismo administrativo independiente» que realiza una revisión previa de las solicitudes de acceso, y que este sistema se ve reforzado por otros niveles adicionales de supervisión judicial a través del juez designado, del procedimiento para la presentación de demandas y del control jurisdiccional.

13 Los demandados alegan asimismo que si, en última instancia, la Ley de 2011 se considerase contraria al Derecho de la Unión, cualquier resolución que emitiese este Tribunal al respecto solo podría tener efectos *a posteriori*. A su modo de ver, en las excepcionales circunstancias del presente asunto, tal solución sería la adecuada, dado que, en el momento en que se tuvo acceso a los datos en el litigio principal, a finales de 2013, el Estado, en virtud del Derecho de la Unión, estaba obligado a cumplir las disposiciones de la Directiva de 2006 y a mantener un sistema de conservación de datos del tipo del establecido en la Ley de 2011. Por otra parte, el Estado argumenta que ello sería lo adecuado en unas circunstancias en las que una declaración de incompatibilidad con el Derecho de la Unión, sin ninguna limitación en sus efectos, tendría importantes consecuencias para la investigación y el enjuiciamiento de delitos graves en Irlanda, respecto de quienes han sido juzgados y condenados y de las investigaciones y los procesos penales que estén en curso.

Breve exposición de la fundamentación de la petición de decisión prejudicial

14 La presente petición de decisión prejudicial busca que se esclarezcan los requisitos del Derecho de la Unión para la conservación de datos con la finalidad

DOCUMENTO DE TRABAJO

de combatir los delitos graves y las necesarias garantías que deben regular el acceso a los mismos, teniendo en cuenta que la competencia en materia penal corresponde a los Estados miembros. Asimismo, el órgano jurisdiccional remitente desea que se dilucide el alcance y los efectos temporales de la resolución instada que, en su caso, pudiera emitirse en las circunstancias del presente asunto.

15 El Supreme Court (Tribunal Supremo) señala que la Ley de 2011 contemplaba la conservación de todos los metadatos con arreglo a sus propios términos, como al parecer era exigible en aquel momento conforme al Derecho de la Unión. No obstante, si, como alega G. D., no puede admitirse la conservación universal de datos en sí misma, entonces la Ley de 2011 es contraria al Derecho de la Unión. Si, por otra parte, como sostiene el Estado, procede acudir a un planteamiento más amplio, habría que tener en cuenta los objetivos del régimen en su conjunto y las circunstancias en las que se permite el acceso y determinar si la Ley de 2011 interfiere de manera proporcionada en los derechos de privacidad garantizados tanto por el Derecho de la Unión Europea como por la Carta de los Derechos Fundamentales de la Unión Europea.

16 El Supreme Court (Tribunal Supremo) reconoce que la cuestión de la admisión de la prueba en los juicios penales es una materia que corresponde al Derecho nacional. Sin embargo, la cuestión de la validez de ciertas partes de la Ley de 2011 es un asunto que puede plantearse en un procedimiento civil. Por otra parte, la cuestión de la referida admisibilidad debería solucionarse a la luz de una declaración de invalidez, si la hubiera, y teniendo en cuenta su naturaleza, su amplitud y su fundamentación, así como su alcance y sus efectos temporales precisos.

17 Por consiguiente, el órgano jurisdiccional remitente considera necesario plantear al TJUE las presentes cuestiones prejudiciales.

DOCUMENTO DE TRABAJO