Recopilación de la Jurisprudencia

Asuntos acumulados C-203/15 y C-698/15

Tele2 Sverige AB
contra
Post- och telestyrelsen
y

Secretary of State for the Home Department
contra
Tom Watson y otros

[Peticiones de decisión prejudicial planteadas por el Kammarrätten i Stockholm y la Court of Appeal (England & Wales) (Civil Division)]

«Procedimiento prejudicial — Comunicaciones electrónicas — Tratamiento de datos personales — Confidencialidad de las comunicaciones electrónicas — Protección — Directiva 2002/58/CE — Artículos 5, 6, 9 y 15, apartado 1 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8, 11 y 52, apartado 1 — Legislación nacional — Proveedores de servicios de comunicaciones electrónicas — Obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización — Autoridades nacionales — Acceso a los datos — Falta de control previo por un órgano jurisdiccional o una autoridad administrativa independiente — Compatibilidad con el Derecho de la Unión»

Sumario — Sentencia del Tribunal de Justicia (Gran Sala) de 21 de diciembre de 2016

1. *Aproximación de las legislaciones — Sector de las telecomunicaciones — Tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Facultad de los Estados miembros de limitar el alcance de determinados derechos y obligaciones — Ámbito de aplicación — Medida legislativa que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar los datos de tráfico y de localización de los usuarios — Inclusión*

   (Directiva 2002/58/CE del Parlamento Europeo y del Consejo, en su versión modificada por la Directiva 2009/136/CE, arts. 5, ap. 1, y 15, ap. 1)

2. *Aproximación de las legislaciones — Sector de las telecomunicaciones — Tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Facultad de los Estados miembros de limitar el alcance de determinados derechos y obligaciones — Interpretación estricta — Motivos que pueden justificar la adopción de una limitación — Carácter exhaustivo*

   (Directiva 2002/58/CE del Parlamento Europeo y del Consejo, en su versión modificada por la Directiva 2009/136/CE, arts. 5, ap. 1, y 15, ap. 1)

3. *Aproximación de las legislaciones — Sector de las telecomunicaciones — Tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Facultad de los Estados miembros de limitar el alcance de determinados derechos y obligaciones — Normativa nacional que prevé la conservación generalizada e indiferenciada de los datos de tráfico y de localización de los usuarios a efectos de la lucha contra la delincuencia — Improcedencia — Injerencia grave en el derecho a la intimidad, a la protección de los datos personales y a la libertad de expresión*

   (Carta de los Derechos Fundamentales de la Unión Europea, arts. 7, 8, 11 y 52, ap. 1; Directiva 2002/58/CE del Parlamento Europeo y del Consejo, en su versión modificada por la Directiva 2009/136/CE, art. 15, ap. 1)

4. *Aproximación de las legislaciones — Sector de las telecomunicaciones — Tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Facultad de los Estados miembros de limitar el alcance de determinados derechos y obligaciones — Normativa nacional que permite la conservación selectiva de los datos de tráfico y de localización de los usuarios a efectos de la lucha contra la delincuencia — Procedencia — Requisitos*

   (Carta de los Derechos Fundamentales de la Unión Europea, arts. 7, 8, 11 y 52, ap. 1; Directiva 2002/58/CE del Parlamento Europeo y del Consejo, en su versión modificada por la Directiva 2009/136/CE, art. 15, ap. 1)

5. *Aproximación de las legislaciones — Sector de las telecomunicaciones — Tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Facultad de los Estados miembros de limitar el alcance de determinados derechos y obligaciones — Normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización de los usuarios — Posibilidad de las autoridades nacionales de acceder a dichos datos sin control judicial o administrativo previo — Improcedencia — Inexistencia de obligación de los proveedores de servicios de comunicaciones electrónicas de conservar esos datos en el territorio de la Unión — Improcedencia*

   (Carta de los Derechos Fundamentales de la Unión Europea, arts. 7, 8, 11 y 52, ap. 1; Directivas del Parlamento Europeo y del Consejo 95/46/CE, art. 22, y 2002/58/CE, en su versión modificada por la Directiva 2009/136/CE, art. 15, aps. 1 y 2)

6. *Derechos fundamentales — Convenio Europeo de los Derechos Humanos — Instrumento no formalmente integrado en el ordenamiento jurídico de la Unión*

   (Art. 6 TUE, ap. 3; Carta de los Derechos Fundamentales de la Unión Europea, art. 52, ap. 3)

7. *Cuestiones prejudiciales — Competencia del Tribunal de Justicia — Límites — Cuestiones generales o hipotéticas — Cuestión que presenta un carácter abstracto y puramente hipotético en relación con el objeto del litigio principal — Inadmisibilidad*

   (Art. 267 TFUE)

1. El artículo 15, apartado 1, de la Directiva 2002/58, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136, autoriza a los Estados miembros a adoptar, respetando los requisitos establecidos en él, medidas legales para limitar el alcance de los derechos y las obligaciones previstas en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de dicha Directiva.

En particular, queda comprendida en el ámbito de aplicación de la citada disposición una medida legal que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar los datos de tráfico y de localización, puesto que dicha actividad implica necesariamente el tratamiento, por ellos, de datos personales. También está incluida en ese ámbito de aplicación una medida legal que regula el acceso de las autoridades nacionales a los datos conservados por dichos proveedores. En efecto, la protección de la confidencialidad de las comunicaciones electrónicas y de sus datos de tráfico, garantizada por el artículo 5, apartado 1, de la Directiva 2002/58, se aplica a las medidas adoptadas por todas las personas distintas de los usuarios, ya sean personas físicas o entidades privadas o públicas.

(véanse los apartados 71 y 75 a 77)

2. El artículo 15, apartado 1, de la Directiva 2002/58, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136, permite a los Estados miembros establecer excepciones a la obligación de principio, enunciada en el artículo 5, apartado 1, de esta Directiva, de garantizar la confidencialidad de los datos personales y a las obligaciones correspondientes, mencionadas concretamente en los artículos 6 y 9 de dicha Directiva. No obstante, puesto que el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros limitar el alcance de dicha obligación de principio, debe interpretarse en sentido estricto. Por tanto, esta disposición no puede justificar que la excepción a dicha obligación de principio y, en particular, a la prohibición de almacenar datos, prevista en el artículo 5 de dicha Directiva, se convierta en la regla si no se quiere privar en gran medida a esta última disposición de su alcance.

A este respecto, el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 prevé que las medidas legales a las que se refiere, y que suponen una excepción al principio de confidencialidad de las comunicaciones y de los datos de tráfico relativos a ellas, deben tener como finalidad proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa y la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o de la utilización no autorizada del sistema de comunicaciones electrónicas, o deben perseguir alguno de los demás objetivos contemplados en el artículo 13, apartado 1, de la Directiva 95/46, 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. Dicha enumeración de objetivos tiene carácter exhaustivo, como se deriva del artículo 15, apartado 1, segunda frase, de esta última Directiva, a cuyo tenor las medidas legales deben estar justificadas por alguno de los motivos establecidos en el artículo 15, apartado 1, primera frase, de dicha Directiva. Por tanto, los Estados miembros no podrán adoptar tales medidas con fines distintos de los enumerados en esta última disposición.

(véanse los apartados 88 a 90)

3. El artículo 15, apartado 1, de la Directiva 2002/58, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136, 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 se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.

En efecto, estos datos, considerados en su conjunto, permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, 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. En particular, estos datos proporcionan medios para determinar el perfil de las personas afectadas, información tan sensible, a la

luz del respeto de la vida privada, como el propio contenido de las comunicaciones. La injerencia que supone una normativa de este tipo en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta tiene una gran magnitud y debe considerarse especialmente grave. El hecho de que la conservación de los datos se efectúe sin que los usuarios de los servicios de comunicaciones electrónicas hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante. Aunque tal normativa no autorice la conservación del contenido de las comunicaciones ni pueda, por tanto, vulnerar el contenido esencial de esos derechos, la conservación de los datos de tráfico y de localización podría, no obstante, influir en el uso de los medios de comunicación electrónica y, en consecuencia, en el ejercicio por los usuarios de esos medios de su libertad de expresión, garantizada por el artículo 11 de la Carta.

Habida cuenta de la gravedad de la injerencia en los derechos fundamentales afectados que supone una normativa nacional como ésta, sólo la lucha contra la delincuencia grave puede justificar una medida de este tipo. No obstante, si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha. Por una parte, una normativa de este tipo tiene como consecuencia que la conservación de los datos de tráfico y de localización se convierta en la regla, mientras que el sistema creado por la Directiva 2002/58 exige que esa conservación de datos sea excepcional. Por otra parte, una normativa nacional de este tipo que cubre de manera generalizada a todos los abonados y usuarios registrados y que tiene por objeto todos los medios de comunicación electrónica así como todos los datos de tráfico no establece ninguna diferenciación, limitación o excepción en función del objetivo que se pretende lograr. Esa normativa se aplica incluso a las personas de las que no existe ningún indicio para pensar que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves. Una normativa nacional de este tipo excede, por tanto, los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta.

(véanse los apartados 99 a 105, 107 y 112 y el punto 1 del fallo)

4. El artículo 15, apartado 1, de la Directiva 2002/58, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136, interpretada a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, no se opone a que un Estado miembro adopte una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido.

Para cumplir esos requisitos, dicha normativa nacional debe establecer, en primer lugar, normas claras y precisas que regulen el alcance y la aplicación de una medida de conservación de datos de este tipo y que prevean unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a los riesgos de abuso. Debe indicar, en particular, en qué circunstancias y con arreglo a qué requisitos puede adoptarse, con carácter preventivo, una medida de conservación de datos, garantizando que tal medida se limite a lo estrictamente necesario.

En segundo lugar, en relación con los requisitos materiales que debe cumplir una normativa nacional de este tipo, para garantizar que se limita a lo estrictamente necesario, si bien tales requisitos pueden variar en función de las medidas adoptadas a efectos de la prevención, investigación, descubrimiento y persecución de la delincuencia grave, la conservación de los datos debe responder en todo caso a criterios objetivos y debe existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr. En particular, tales requisitos deben permitir que pueda delimitarse en la práctica de modo efectivo el alcance de la medida y, en consecuencia, el público afectado. Por lo que se refiere a esta delimitación, la normativa nacional debe basarse en elementos objetivos que permitan dirigirse a un público cuyos datos puedan presentar una relación, por lo menos indirecta, con delitos graves, contribuir de un modo u otro a la lucha contra la delincuencia grave o prevenir un riesgo grave para la seguridad pública. Tal delimitación puede garantizarse mediante un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de elementos objetivos, que existe un riesgo elevado de preparación o de comisión de tales delitos en una o varias zonas geográficas.

(véanse los apartados 108 a 111)

5. El artículo 15, apartado 1, de la Directiva 2002/58, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136, 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 se opone a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trate se conserven en el territorio de la Unión.

A este respecto, para garantizar que el acceso de las autoridades nacionales competentes a los datos conservados se limite a lo estrictamente necesario, es ciertamente el Derecho nacional el que debe determinar los requisitos conforme a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder dicho acceso. No obstante, la normativa nacional de que se trate no puede limitarse a exigir que el acceso responda a alguno de los objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, ni siquiera el de la lucha contra la delincuencia grave. En efecto, tal normativa nacional debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados. De este modo, y puesto que un acceso general a todos los datos conservados, con independencia de la existencia de una relación, por lo menos indirecta, con el fin perseguido, no puede considerarse limitado a lo estrictamente necesario, la normativa nacional de que se trate debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos de los abonados o usuarios registrados. A este respecto, en principio sólo podrá concederse un acceso en relación con el objetivo de la lucha contra la delincuencia a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave. No obstante, en situaciones particulares, como aquellas en las que intereses vitales de la seguridad nacional, la defensa o la seguridad pública están amenazados por actividades terroristas, podría igualmente concederse el acceso a los datos de otras personas cuando existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra dichas actividades.

Para garantizar en la práctica el pleno cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se produzca a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco

de procedimientos de prevención, descubrimiento o acciones penales. Del mismo modo, es necesario que las autoridades nacionales competentes a las que se conceda el acceso a los datos conservados informen de ello a las personas afectadas, en el marco de los procedimientos nacionales aplicables, siempre que esa comunicación no pueda comprometer las investigaciones que llevan a cabo esas autoridades. En efecto, esa información es, de hecho, necesaria para que dichas personas puedan ejercer, concretamente, su derecho a la tutela judicial efectiva, previsto expresamente en el artículo 15, apartado 2, de la Directiva 2002/58, en relación con el artículo 22 de la Directiva 95/46, 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, en caso de vulneración de sus derechos.

Además, habida cuenta de la cantidad de datos conservados, del carácter sensible de esos datos y del riesgo de acceso ilícito a éstos, los proveedores de servicios de comunicaciones electrónicas deben garantizar, para asegurar la plena integridad y confidencialidad de esos datos, un nivel particularmente elevado de protección y de seguridad mediante medidas técnicas y de gestión adecuadas. En particular, la normativa nacional debe prever la conservación de los datos en el territorio de la Unión y la destrucción definitiva de los datos al término del período de conservación de éstos.

(véanse los apartados 118 a 122 y 125 y el punto 2 del fallo)

6. Véase el texto de la resolución.

(véanse los apartados 127 a 129)

7. Véase el texto de la resolución.

(véase el apartado 130)