



Prensa e Información

Tribunal de Justicia de la Unión Europea
COMUNICADO DE PRENSA n.º 145/16

Luxemburgo, 21 de diciembre de 2016

Sentencia en los asuntos acumulados C-203/15
Tele2 Sverige AB / Post- och telestyrelsen y C-698/15 Secretary of State for
the Home Department/Tom Watson y otros

Los Estados miembros no pueden imponer una obligación general de conservación de datos a los proveedores de servicios de comunicaciones electrónicas

El Derecho de la Unión se opone a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, pero los Estados miembros podrán establecer, con carácter preventivo, una conservación selectiva de esos datos con la única finalidad de luchar contra la delincuencia grave, siempre que tal conservación se limite a lo estrictamente necesario por lo que se refiere a las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido. El acceso de las autoridades nacionales a los datos conservados debe estar sujeto a requisitos, entre los que se encuentran en particular un control previo por una autoridad independiente y la conservación de los datos en el territorio de la Unión

En su sentencia *Digital Rights Ireland* de 2014,¹ el Tribunal de Justicia declaró la invalidez de la Directiva relativa a la conservación de datos² debido a que la injerencia que supone la obligación general de conservar datos de tráfico y de localización, impuesta por ésta, en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales no estaba limitada a lo estrictamente necesario.

A raíz de dicha sentencia, se plantearon ante el Tribunal de Justicia dos asuntos en relación con la obligación general impuesta, en Suecia y en el Reino Unido, a los proveedores de servicios de comunicaciones electrónicas de conservar los datos relativos a las comunicaciones, cuya conservación estaba prevista por la Directiva invalidada.

Al día siguiente del pronunciamiento de la sentencia *Digital Rights Ireland*, la empresa de telecomunicación Tele2 Sverige notificó a la autoridad sueca de control de los servicios de correos y telecomunicaciones su decisión de no seguir conservando los datos y su intención de suprimir los datos ya registrados (asunto C-203/15). El Derecho sueco obliga en efecto a los proveedores de servicios de comunicaciones electrónicas a conservar de modo sistemático y continuado, sin ninguna excepción, todos los datos de tráfico y de localización de todos sus abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.

En el asunto C-698/15, los Sres. Tom Watson, Peter Brice y Geoffrey Lewis interpusieron recursos contra la normativa británica de conservación de datos que permite al Ministro del Interior obligar a los operadores de telecomunicaciones públicas a conservar todos los datos relativos a las comunicaciones durante un período máximo de doce meses, estando excluida la conservación del contenido de esas comunicaciones.

El Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo, Suecia) y la Court of Appeal (England and Wales) (Civil Division) [Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil), Reino Unido] solicitan al Tribunal de Justicia que indique si las normativas nacionales que imponen a los proveedores una obligación

¹ Sentencia del Tribunal de Justicia de 8 de abril de 2014, *Digital Rights Ireland y Seitlinger y otros* (asuntos acumulados C-293/12 y C-594/12, véase CP n.º 54/14).

² 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 L 105, p. 54).

general de conservación de datos y que prevén el acceso de las autoridades nacionales competentes a los datos conservados sin limitar este acceso a los casos de lucha contra la delincuencia grave y sin supeditar el acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, son compatibles con el Derecho de la Unión (en el presente caso, la Directiva sobre la privacidad y las comunicaciones electrónicas,³ interpretada a la luz de la Carta de los Derechos Fundamentales de la UE).⁴

En la sentencia que se dicta hoy, **el Tribunal de Justicia responde que el Derecho de la Unión se opone a una normativa nacional que establece la conservación generalizada e indiferenciada de los datos.**

El Tribunal de Justicia confirma, en primer lugar, que **las medidas nacionales** controvertidas **están comprendidas en el ámbito de aplicación de la Directiva.** En efecto, la protección de la confidencialidad de las comunicaciones electrónicas y de los datos de tráfico, garantizada por la Directiva, se aplica a las medidas adoptadas por toda persona distinta de los usuarios, ya sean personas físicas o entidades privadas o públicas.

El Tribunal de Justicia declara, a continuación, que, si bien dicha Directiva permite a los Estados miembros limitar el alcance de la obligación de principio de garantizar la confidencialidad de las comunicaciones y de los datos de tráfico relativos a ellas, no puede justificar que la excepción a esta obligación de principio y, en particular, a la prohibición de almacenar esos datos, prevista en ella, se convierta en la regla.

Además, el Tribunal de Justicia recuerda su reiterada jurisprudencia conforme a la cual la protección del derecho fundamental al respeto de la vida privada exige que **las excepciones** a la protección de los datos personales **no excedan de lo estrictamente necesario.** El Tribunal de Justicia aplica esta jurisprudencia a las normas que regulan la conservación de datos y a las que regulan el acceso a los datos conservados.

El Tribunal de Justicia señala, **por lo que se refiere a la conservación,** que los datos conservados considerados en su conjunto **permiten extraer conclusiones muy precisas sobre la vida privada de las personas** cuyos datos se han conservado.

Por tanto, **la injerencia que resulta de una normativa nacional que establece la conservación de los datos de tráfico y de localización 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. En consecuencia, **sólo la lucha contra la delincuencia grave puede justificar tal injerencia.**

El Tribunal de Justicia señala que una **normativa que establece la conservación generalizada e indiferenciada de los datos no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública** y no se limita, en particular, a prever una conservación de datos referentes a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas en un delito grave. **Tal normativa nacional excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige la Directiva, interpretada a la luz de la Carta.**

El Tribunal de Justicia aclara, en cambio, que **la Directiva no se opone a una normativa nacional que imponga la conservación selectiva de datos** con la finalidad de luchar contra la delincuencia grave, **siempre que tal conservación 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. Según el

³ 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 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 L 337, p. 11).

⁴ Artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea.

Tribunal de Justicia, **toda normativa nacional que vaya en este sentido debe ser clara y precisa y prever garantías suficientes** a fin de proteger los datos frente a los riesgos de abuso. Debe indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse, con carácter preventivo, una medida de conservación de datos, de modo que se garantice el alcance de esta medida esté efectivamente limitado, en la práctica, a lo estrictamente necesario. En particular, tal normativa debe **basarse en elementos objetivos** que permitan dirigirse a las personas cuyos datos puedan presentar una relación con delitos graves, contribuir a la lucha contra la delincuencia grave o prevenir un riesgo grave para la seguridad pública.

Por lo que se refiere al **acceso de las autoridades nacionales competentes a los datos conservados**, el Tribunal de Justicia confirma que la normativa nacional de que se trata no puede limitarse a exigir que el acceso responda a alguno de los objetivos contemplados en la Directiva, ni siquiera el de la lucha contra la delincuencia grave, sino que debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados. Esta normativa 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**. 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 estén 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 tales actividades.

Además, el Tribunal de Justicia considera que **es esencial que el acceso a los datos conservados esté sujeto, salvo en caso de urgencia, a un control previo** de un órgano jurisdiccional o de una entidad independiente. Por otro lado, las autoridades nacionales competentes a las que se conceda el acceso a los datos conservados deberán informar de ello a las personas afectadas.

Habida cuenta de la cantidad de datos conservados, del carácter sensible de esos datos y del riesgo de acceso ilícito a éstos, **la normativa nacional debe prever que los datos se conserven en el territorio de la Unión** y que se destruyan definitivamente al término del período de conservación de éstos.

NOTA: La remisión prejudicial permite que los tribunales de los Estados miembros, en el contexto de un litigio del que estén conociendo, interroguen al Tribunal de Justicia acerca de la interpretación del Derecho de la Unión o sobre la validez de un acto de la Unión. El Tribunal de Justicia no resuelve el litigio nacional, y es el tribunal nacional quien debe resolver el litigio de conformidad con la decisión del Tribunal de Justicia. Dicha decisión vincula igualmente a los demás tribunales nacionales que conozcan de un problema similar.

Documento no oficial, destinado a los medios de comunicación y que no vincula al Tribunal de Justicia.

El [texto íntegro](#) de la sentencia se publica en el sitio CURIA el día de su pronunciamiento.

Contactos con la prensa: Liliane Fonseca Almeida ☎ (+352) 4303 3667

Las imágenes del pronunciamiento de la sentencia se encuentran disponibles en

«[Europe by Satellite](#)» ☎ (+32) 2 2964106