



Prensa e Información

Tribunal de Justicia de la Unión Europea

**COMUNICADO DE PRENSA n.º 29/21**

Luxemburgo, 2 de marzo de 2021

Sentencia en el asunto C-746/18

H. K/Prokuratuur

**El acceso, a efectos penales, a un conjunto de datos de comunicaciones electrónicas de tráfico o de localización que permiten llegar a conclusiones precisas sobre la vida privada solo se autoriza para luchar contra la delincuencia grave y prevenir las amenazas graves contra la seguridad pública**

*Por otra parte, el Derecho de la Unión se opone a una normativa nacional que atribuye competencia al Ministerio Fiscal para autorizar el acceso de una autoridad pública a esos datos con el fin de hacer la instrucción penal*

En Estonia se incoó un proceso penal contra H. K. por los cargos de robo, utilización de la tarjeta bancaria de un tercero y violencia contra los intervinientes en un procedimiento judicial. Por estos delitos, H. K. fue condenada por un tribunal de primera instancia a una pena privativa de libertad de dos años, sentencia que fue posteriormente confirmada en apelación.

Los atestados en los que se basa la apreciación de esos delitos fueron redactados, en particular, sobre la base de datos personales generados en el marco de la prestación de servicios de comunicaciones electrónicas. El Riigikohus (Tribunal Supremo, Estonia), ante el que H. K. interpuso un recurso de casación, albergaba dudas en cuanto a la compatibilidad con el Derecho de la Unión <sup>1</sup> de las condiciones en las que los servicios de investigación tuvieron acceso a esos datos.

Estas dudas se refieren, en primer lugar, a si la duración del período en el que los servicios de investigación tuvieron acceso a los datos constituye un criterio que permite evaluar la gravedad de la injerencia de dicho acceso en los derechos fundamentales de las personas afectadas. Así, cuando ese período es muy breve o la cantidad de datos recogidos es muy limitada, el Riigikohus se preguntaba si el objetivo de lucha contra la delincuencia en general, y no solo de lucha contra la delincuencia grave, puede justificar tal injerencia. En segundo lugar, el Riigikohus albergaba dudas sobre la posibilidad de considerar al Ministerio Fiscal estonio, habida cuenta de las distintas funciones que le atribuye la normativa nacional, una autoridad administrativa «independiente», en el sentido de la sentencia *Tele2 Sverige y Watson y otros*, <sup>2</sup> que pueda autorizar el acceso de la autoridad investigadora a los datos en cuestión.

Mediante su sentencia, pronunciada en Gran Sala, **el Tribunal de Justicia declara que la Directiva sobre la privacidad y las comunicaciones electrónicas, en relación con la Carta, se opone a una normativa nacional que autoriza el acceso de las autoridades públicas a datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y permitir llegar a conclusiones**

<sup>1</sup> Más concretamente, con 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 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 sobre la privacidad y las comunicaciones electrónicas»), en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

<sup>2</sup> Sentencia de 21 de diciembre de 2016, *Tele2 Sverige y Watson y otros*, [C-203/15](#) y [C-698/15](#), apartado 120; véase también el comunicado de prensa n.º [145/16](#).

**precisas sobre su vida privada, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, sin que dicho acceso se limite a procedimientos que tengan por objeto la lucha contra la delincuencia grave o la prevención de amenazas graves contra la seguridad pública. Según el Tribunal de Justicia, la duración del período para el que se solicite acceder a esos datos y la cantidad o naturaleza de los datos disponibles en ese período es irrelevante al respecto. Además, el Tribunal de Justicia considera que esa Directiva, en relación con la Carta, se opone a una normativa nacional que atribuye al Ministerio Fiscal competencia para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización con el fin de realizar la instrucción penal.**

#### Apreciación del Tribunal de Justicia

Por lo que respecta a las condiciones en las que puede concederse el acceso a los datos de tráfico y de localización conservados por los proveedores de servicios de comunicaciones electrónicas, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, a las autoridades públicas con arreglo a una medida adoptada al amparo de la Directiva sobre la privacidad y las comunicaciones electrónicas,<sup>3</sup> el Tribunal de Justicia recuerda lo que declaró en su sentencia *La Quadrature du Net y otros*.<sup>4</sup> Así, esta Directiva únicamente autoriza a los Estados miembros a adoptar —entre otros, a esos fines— medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en dicha Directiva, en particular la obligación de garantizar la confidencialidad de las comunicaciones y de los datos de tráfico,<sup>5</sup> respetando los principios generales del Derecho de la Unión —entre los que figura el principio de proporcionalidad— y los derechos fundamentales garantizados por la Carta.<sup>6</sup> En este contexto, la Directiva se opone a medidas legislativas que impongan a los proveedores de servicios de comunicaciones electrónicas, con carácter preventivo, la conservación generalizada e indiferenciada de los datos de tráfico y de localización.

En lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos pretendido por la normativa controvertida, de conformidad con el principio de proporcionalidad, el Tribunal de Justicia considera que solo los objetivos de lucha contra la delincuencia grave o de prevención de las amenazas graves contra la seguridad pública pueden justificar el acceso de las autoridades públicas a un conjunto de datos de tráfico o de localización que puedan permitir extraer conclusiones precisas sobre la vida privada de las personas afectadas, sin que otros factores relativos a la proporcionalidad de la solicitud de acceso, como la duración del período para el que se solicita el acceso a dichos datos, puedan conllevar que el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general justifique tal acceso.

Por lo que respecta a la competencia atribuida al Ministerio Fiscal para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización con el fin de dirigir la instrucción penal, el Tribunal de Justicia recuerda que corresponde al Derecho nacional determinar los requisitos con arreglo a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos de que disponen. No obstante, para cumplir el requisito de proporcionalidad, una normativa de este tipo debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger de manera eficaz esos datos contra los riesgos de abuso. Dicha normativa debe ser legalmente imperativa en Derecho interno e indicar en qué circunstancias y con arreglo a qué requisitos materiales y procedimentales puede adoptarse una medida que contemple el tratamiento de esos datos, garantizando así que la injerencia se limite a lo estrictamente necesario.

Según el Tribunal de Justicia, para garantizar en la práctica el íntegro cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos

<sup>3</sup> Artículo 15, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

<sup>4</sup> Sentencia de 6 de octubre de 2020, *La Quadrature du Net y otros*, [C-511/18](#), [C-512/18](#) y [C-520/18](#), apartados 166 a 169; véase también el comunicado de prensa n.º [123/20](#).

<sup>5</sup> Artículo 5, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

<sup>6</sup> En concreto, los artículos 7, 8, 11 y 52, apartado 1, de la Carta.

conservados se supedita a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se dicte a raíz de una solicitud motivada de dichas autoridades presentada, en particular, en el marco de procedimientos de prevención, descubrimiento y persecución de delitos. En caso de urgencia debidamente justificada, el control debe efectuarse en breve plazo.

A este respecto, el Tribunal de Justicia precisa que el control previo requiere, entre otras cosas, que el órgano jurisdiccional o la entidad encargada de efectuar dicho control dispongan de todas las atribuciones y presenten todas las garantías necesarias para conciliar los diferentes intereses y derechos de que se trate. En el caso concreto de la investigación penal, este control exige que ese órgano jurisdiccional o esa entidad estén en condiciones de ponderar adecuadamente, por una parte, los intereses relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de aquellos a cuyos datos afecte el acceso. Cuando dicho control no lo lleve a cabo un órgano jurisdiccional, sino una entidad administrativa independiente, esta debe gozar de un estatuto que le permita actuar en el ejercicio de sus funciones con objetividad e imparcialidad, y, para ello, ha de estar a resguardo de toda influencia externa.

Según el Tribunal de Justicia, de ello resulta que el requisito de independencia que debe cumplir la autoridad que ejerce el control previo obliga a que dicha autoridad tenga la condición de tercero respecto de la que solicita el acceso a los datos, de modo que la primera pueda ejercer ese control con objetividad e imparcialidad, y a resguardo de toda influencia externa. En particular, en el ámbito penal, el requisito de independencia implica que la autoridad que ejerce ese control previo, por una parte, no esté implicada en la realización de la investigación penal de que se trate y, por otra parte, que tenga una posición neutral frente a las partes del procedimiento penal. Sin embargo, no ocurre así con un Ministerio Fiscal, como el Ministerio Fiscal estonio, que dirige el procedimiento de investigación y ejerce, en su caso, la acusación pública. De ello se deduce que el Ministerio Fiscal no puede llevar a cabo ese control previo.

---

**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: Cristina López Roca ☎ (+352) 4303 3667*

*Las imágenes del pronunciamiento de la sentencia se encuentran disponibles en*

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