

Telecomunicaciones

Límites a la obligación de los operadores de telecomunicaciones de conservar los datos de tráfico y localización para la persecución de actos ilícitos

Los operadores de telecomunicaciones no están obligados a conservar datos de tráfico y localización para la lucha disciplinaria contra la corrupción.

ANA I. MENDOZA LOSANA

Profesora titular de Derecho Civil de la Universidad de Castilla-La Mancha
Consejera académica de Gómez-Acebo & Pombo

La Sentencia del Tribunal de Justicia de la Unión Europea de 7 de septiembre del 2023, asunto C-162/22, *Lietuvos Respublikos generalinė prokuratūra* (ECLI: ES:EUC:2023:631), se suma al numeroso conjunto de sentencias del citado tribunal que se pronuncia sobre el alcance de la obligación de los operadores de telecomunicaciones de conservar los datos de tráfico y de localización. Esta obligación deriva del artículo 15, apartado 1, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, 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/CE del Parlamento Europeo y del Consejo, de 25 de noviembre

(en lo sucesivo, «Directiva 2002/58»). Dicho precepto permite a los Estados establecer medidas legislativas que restrinjan derechos fundamentales como el derecho al secreto de las comunicaciones y la protección de los datos personales y obliguen a los operadores de telecomunicaciones a conservar los datos generados por las comunicaciones electrónicas para la consecución de los objetivos de interés general enumerados en la directiva, entre otros, la persecución de delitos graves.

1. Hechos

En el proceso que da origen a la cuestión prejudicial se solicitó la nulidad de dos resoluciones de la fiscalía general de Lituania en las que se sancionó y suspendió de sus funciones

a un fiscal por haber facilitado ilegalmente información a un sospechoso y a su abogado durante una instrucción. La conducta que dio lugar a la sanción disciplinaria se acreditó gracias a los datos conservados por los proveedores de servicios de comunicaciones electrónicas. En concreto, consta la existencia de sendos autos judiciales en los que se había autorizado la interceptación y la grabación de la información transmitida a través de las redes de comunicaciones electrónicas relativas al abogado en cuestión y al demandante en el litigio principal. No obstante, una vez que se obtuvieron esos datos, se utilizaron para un procedimiento administrativo que no era el proceso penal en el marco del cual se ordenó la interceptación de las comunicaciones y la correlativa conservación y cesión de datos.

2. **Cuestión prejudicial: acceso y uso de datos de tráfico y localización en procesos no penales**

En el caso se cuestionaba si los datos conservados y facilitados por los operadores para perseguir delitos podrían ser utilizados también en un procedimiento disciplinario para depurar las responsabilidades derivadas de un ejercicio inadecuado del cargo. Entre otros, se somete a la consideración del Tribunal de Justicia de la Unión Europea el artículo 19, apartado 1, punto 5, de la Ley lituana de Inteligencia Criminal, según el cual, la información procedente de operaciones de investigación criminal relativa a un hecho que presente las características de una infracción relacionada con la corrupción podrá ser desclasificada, previo acuerdo del ministerio fiscal, y utilizada en el marco de una investigación sobre faltas disciplinarias o en el ejercicio del cargo.

En el litigio principal, el demandante (fiscal apartado) diferenciaba dos elementos: a) el

acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas con fines distintos de la lucha contra las infracciones graves y la prevención de las amenazas graves contra la seguridad pública; b) una vez obtenido dicho acceso, la utilización de esos datos para investigar conductas indebidas en el ejercicio del cargo relacionadas con la corrupción. Según el demandante, la utilización de datos que permiten identificar el origen y el destino de una comunicación telefónica desde el teléfono fijo o móvil de un investigado en procedimientos relacionados con una conducta indebida en el ejercicio del cargo (no en causas penales ni relacionadas directamente con la comisión de delitos graves) constituiría una injerencia injustificada en los derechos fundamentales contraria el Derecho de la Unión.

El órgano jurisdiccional nacional, que ha de pronunciarse sobre la nulidad de las resoluciones impugnadas, cuestiona si el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7 (derecho a la privacidad de las comunicaciones), 8 (protección de datos de carácter personal), 11 (libertad de expresión) y 52, apartado 1 (límites al ejercicio de derechos y libertades conforme al principio de proporcionalidad), de la Carta de los Derechos Fundamentales de la Unión Europea debe interpretarse en el sentido de que se opone a que, en investigaciones relativas a conductas indebidas en el ejercicio del cargo relacionadas con la corrupción, se puedan utilizar datos personales relativos a comunicaciones electrónicas que, en aplicación de una medida legislativa adoptada en virtud de dicho artículo, hayan sido conservados por los proveedores de servicios de comunicaciones electrónicas y que posteriormente, en aplicación de dicha medida, se hayan puesto a disposición de las autoridades competentes a efectos de la lucha contra la delincuencia grave.

Obsérvese el matiz diferencial: no se cuestiona el acceso a los datos (que en el caso se ha producido con la finalidad de perseguir delitos graves en el marco de una investigación criminal y con la correspondiente autorización), sino el uso dado a aquellos datos (se han utilizado para sancionar conductas relacionadas con la corrupción en el ejercicio de un cargo).

3. Algunas consideraciones previas sobre el deber de los operadores de conservación (indiscriminada) de datos de tráfico y localización

Aunque no es objeto de la sentencia cuestionada, dadas las numerosas dudas doctrinales y jurisprudenciales que está suscitando la obligación impuesta a los operadores de comunicaciones electrónicas de conservar los datos de tráfico y localización durante un tiempo determinado, se considera necesario recordar aquí la situación jurídica en la que se encuentra esta cuestión. Tras la anulación por el Tribunal de Justicia de la Unión Europea de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, 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, se han cuestionado numerosas leyes europeas, que, como la española (Ley 25/2007, de 18 octubre, de conservación de datos de comunicaciones electrónicas y de redes públicas de comunicación), imponen a los operadores de comunicaciones electrónicas el deber de conservar datos de tráfico (origen y destino de la comunicación, tipo de terminal utilizado, identidad de los usuarios implicados en la comunicación y direcciones IP) y de localización de todas las comunicaciones realizadas por todos los usuarios de los servicios de comunicaciones electrónicas

durante un tiempo determinado (en España, un año). Este tipo de obligación, en principio, podría calificarse como una conservación generalizada e indiscriminada sólo limitada en el tiempo y constitutiva de un tratamiento de datos de carácter personal ilícito y no justificado por razones de interés general.

Para no alargar en exceso este trabajo, no se reproduce aquí toda la jurisprudencia del Tribunal de Justicia de la Unión Europea que se ha pronunciado sobre esta obligación y sus límites. La propia sentencia glosada recoge en sus fundamentos jurídicos una apretada síntesis de las numerosas sentencias que añaden nuevos matices al deber de conservación y que, en principio, parecen excluir la conservación indiscriminada (véanse, por todas, las sentencias del Tribunal de Justicia de la Unión Europea de 6 de octubre del 2020, *La Quadrature du Net y otros*, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apdo. 110; de 2 de marzo del 2021, *Prokuratuur, Condiciones de acceso a los datos relativos a las comunicaciones electrónicas*, C-746/18, EU:C:2021:152, apdos. 33 y 35; y de 20 de septiembre del 2022, *SpaceNet y Telekom Deutschland*, C-793/19 y C-794/19, EU:C:2022:702, apdos. 74 y 131 y jurisprudencia citada). En cualquier caso y por cuanto constituye una injerencia en los derechos fundamentales, el deber de conservación debe estar sujeto a un estricto régimen de garantías, debe ser interpretado restrictivamente y constituye una excepción que debe estar justificada por razones de interés general y conforme al principio de proporcionalidad (véase la Sentencia del Tribunal de Justicia de la Unión Europea de 5 de abril del 2022, *Commissioner of an Garda Síochána y otros*, C-140/20, EU:C:2022:258, apdo. 40).

En España, la cuestión parece, de momento, estar resuelta por la Sentencia del Tribunal Supremo (Sala de lo Penal, Sección Primera)

núm. 824/2022, de 19 octubre. En esta sentencia, el alto tribunal declina elevar cuestión prejudicial —como solicitaba el recurrente—, recoge la vasta doctrina jurisprudencial existente sobre el deber de conservación (tanto del Tribunal de Justicia de la Unión Europea como del Tribunal Europeo de Derechos Humanos y del propio Tribunal Supremo) y llega a la conclusión de que la obligación de conservación generalizada e indiscriminada de los datos de tráfico y localización durante un año en los términos y con las garantías impuestas en el ordenamiento español no constituye una atentado injustificado contra los derechos fundamentales reconocidos por el Derecho de la Unión. Según el tribunal, se trata de una obligación instrumental e imprescindible para que, llegado el momento y con las debidas garantías —entre otras, la imprescindible autorización judicial—, se pueda facilitar el acceso a las autoridades competentes a los datos conservados para la satisfacción de los objetivos de interés general citados de forma taxativa en la Directiva 2002/58/CE.

4. Doctrina: la persecución de delitos no graves o de faltas disciplinarias no justifica la injerencia en los derechos fundamentales

En esta nueva sentencia de 7 de septiembre del 2023, el Tribunal de Justicia de la Unión Europea completa su doctrina sobre el deber de conservación de datos de tráfico y localización en el marco de la prestación de servicios de comunicaciones electrónicas. En ella, el Tribunal de Justicia de la Unión Europea declara que, conforme al principio de proporcionalidad, sólo la lucha contra la delincuencia grave y la prevención de amenazas graves para la seguridad pública pueden justificar una injerencia grave en los derechos fundamentales como la que supone la conservación de los datos de tráfico y de localización. Los operadores de telecomunicaciones

sólo están obligados a conservar y ceder los datos de tráfico y localización a las autoridades competentes en el marco de un proceso penal y para la lucha contra los delitos graves.

De la sentencia y de la jurisprudencia por ella citada cabe extraer las siguientes reglas:

- 1.^a Dentro del orden jerárquico de los objetivos de interés general enumerados en el artículo 15, apartado 1, de la Directiva 2002/58/CE, conforme al principio de proporcionalidad, la importancia del objetivo de protección de la seguridad nacional (responsabilidad exclusiva de cada Estado miembro) supera a la de los demás objetivos previstos, en particular, a la de los objetivos de combatir la delincuencia en general, incluso grave, y a la de la prevención de amenazas no graves contra la seguridad pública (STJUE de 5 de abril del 2022, *Commissioner of an Garda Síochána* y otros, C-140/20, EU:C:2022:258, apdo. 99).
- 2.^a Correlativamente, el objetivo de protección de la seguridad nacional puede justificar medidas que supongan injerencias en los derechos fundamentales más graves que las que podrían justificar los otros objetivos (STJUE de 5 de abril del 2022, *Commissioner of an Garda Síochána* y otros, C-140/20, EU:C:2022:258, apdo. 57 y jurisprudencia citada).
- 3.^a El objetivo de prevención, investigación, descubrimiento y persecución de delitos en general puede justificar las injerencias en los derechos fundamentales que no presenten un carácter grave (STJUE de 5 de abril del 2022, *Commissioner of an Garda Síochána* y otros, C-140/20, EU:C:2022:258, apdo. 59 y jurisprudencia citada).

El acceso y la utilización de los datos de tráfico y de localización conservados por los proveedores con arreglo a una medida adoptada de conformidad con el artículo 15, apartado 1, de la Directiva 2002/58, sólo puede estar justificado, en principio, por el objetivo de interés general para el que dicha conservación se impuso a estos proveedores. Sólo cabría una solución diferente si la importancia del objetivo perseguido por el acceso fuera mayor que la del objetivo que justificó la conservación (STJUE de 5 de abril del 2022, *Commissioner of an Garda Síochána y otros*, C-140/20, EU:C:2022:258, apdo. 98 y jurisprudencia citada).

- 5.^a El mismo criterio formulado en el apartado anterior ha de aplicarse para otras posibles utilidades de los datos conservados: tras haber sido conservados y puestos a disposición de las autoridades competentes a efectos de la lucha contra la delincuencia grave, tales datos no pueden transmitirse a otras autoridades ni utilizarse para alcanzar objetivos diferentes, aunque éstos sean la lucha contra las conductas indebidas en el ejercicio del cargo relacionadas con la corrupción. Este otro fin es de una importancia menor en la jerarquía de los objetivos de interés general que el de la lucha contra la delincuencia grave y el de la prevención de las amenazas graves contra la seguridad pública. En tal caso, el acceso a los datos conservados sería contrario a la jerarquía de objetivos de interés general referida en los apartados anteriores (véase en este sentido, la STJUE de 5 de abril del 2022, *Commissioner of an Garda Síochána y otros*, C-140/20,

EU:C:2022:258, apdo. 99, y el apdo. 41 de la sentencia considerada).

- 6.^a Un procedimiento disciplinario relativo a conductas indebidas en el ejercicio del cargo relacionadas con la corrupción podría estar relacionado con la protección de la seguridad pública, si bien ello exigiría al interesado probar la existencia de alguna amenaza grave para la seguridad pública (véase el apdo. 42 de la sentencia comentada). No obstante, a la luz del artículo 15.1 de la directiva, la restricción de los derechos fundamentales derivada de la conservación de datos de tráfico y localización sólo está justificada en el marco de un proceso penal y no en el de un procedimiento disciplinario, por muy importante que sea el papel desempeñado por éste en la lucha contra la delincuencia grave (véase el apdo. 43 de la sentencia comentada).

5. Conclusión

El Tribunal de Justicia de la Unión Europea concluye que los datos de tráfico y localización conservados por los proveedores en aplicación de una medida adoptada en virtud del artículo 15.1 de la Directiva 2002/58/CE a efectos de la lucha contra la delincuencia grave no pueden transmitirse posteriormente a otras autoridades ni utilizarse para la lucha contra las conductas indebidas en el ejercicio del cargo relacionadas con la corrupción, que son de una importancia menor que la lucha contra la delincuencia grave. En otros términos, la citada directiva se opone a que los datos recabados a efectos de la lucha contra la delincuencia grave se utilicen en investigaciones administrativas relacionadas con la corrupción en el sector público.