ACCESO A COMUNICACIONES ELECTRÓNICAS Y TRATAMIENTO DE DATOS PERSONALES: NUEVO CRITERIO. COMENTARIO A LA STJUE (GRAN SALA) C-207/16, DE 2 DE OCTUBRE DE 2018, SOBRE ACCESO DE LAS AUTORIDADES NACIONALES A LOS DATOS PARA LA INVESTIGACIÓN DE UN DELITO Y UMBRAL DE GRAVEDAD DEL DELITO QUE PUEDE JUSTIFICAR EL ACCESO A LOS DATOS

Laura Caballero Trenado
Doctora en Ciencias de la Comunicación
Graduada en Derecho
Profesora de la UNIR

Fecha de recepción: 17 de septiembre de 2018
Fecha de aceptación: 29 de octubre de 2018

RESUMEN: El TJUE resuelve en la Sentencia *C-207/16*, de 2 de octubre de 2018, una cuestión prejudicial planteada por una Audiencia Provincial española y aboga por el criterio de proporcionalidad. Conforme a este principio, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de grave. En cambio, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir delitos en general. El TJUE opta aplicar un principio de proporcionalidad para el acceso de las autoridades públicas a los datos que permitan identificar a los titulares de las tarjetas SIM de un móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, al considerar que, el acceso limitado únicamente a los datos cubiertos por la solicitud controvertida no puede calificarse de injerencia grave en los derechos fundamentales de los datos de los investigados cuyos datos se ven comprometidos. En la tesitura entre seguridad y libertad, esta Decisión bascula una ponderación en favor de la primera, lo que implica un cambio de criterio.

ABSTRACT: The CJEU resolves in Judgment C-207/16, of October 2, 2018, a preliminary ruling submitted by a Spanish Provincial Court and advocates the proportionality criterion. In accordance with this principle, in the field of prevention, investigation, discovery and prosecution of crimes, the objective of combating crime, which in turn is also qualified as serious, can justify serious interference. On the other hand, when the interference implied by such access is not serious, it may be justified by the objective of preventing, investigating, discovering and prosecuting crimes in general. The CJEU opts to apply a principle of proportionality for the access of public authorities to the data that allows identifying the holders of the SIM cards of a stolen mobile, such as names, surnames and, where appropriate, the addresses of those holders, considering that access limited only to the data covered by the contested application can not be classified as a serious interference with the fundamental rights of the data of those investigated whose data are compromised. In the position between security and freedom, this Decision tilts a weight in favour of the first, which, therefore, implies an overruling.

PALABRAS CLAVE: Secreto de las comunicaciones; datos personales; principio de proporcionalidad.

KEYWORDS: Secret of Communications; Personal Data; Principle of Proportionality.

1. INTRODUCCIÓN

En apretada síntesis, la presente Sentencia resuelve una cuestión prejudicial[1] planteada por la Audiencia Provincial de Tarragona en abril de 2016.

La cuestión elevada al TJUE por el órgano jurisdiccional español tiene como trasfondo un procedimiento relativo al robo con violencia de un teléfono móvil, donde la Policía Judicial solicitó al juez instructor que se ordenase a diversos proveedores de servicios de comunicaciones la identificación durante un periodo de tiempo concreto de los datos personales de los posibles titulares o usuarios de números correspondientes a la tarjeta SIM del móvil robado relacionadas con el código IMEI de dicho equipo.

Las dudas que el juez instructor plantea al juzgador europeo son las siguientes. En primer término, ¿la suficiente gravedad de los delitos como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta puede identificarse únicamente en atención a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos?

En segundo lugar, si se ajustara a los principios constitucionales de la Unión, utilizados por el [Tribunal de Justicia] en su sentencia de 8 de abril de 2014 [*Digital Rights Ireland* y otros, *C-293/12* y *C-594/12*] como estándares de control estricto de la Directiva, la determinación de la gravedad del delito atendiendo solo a la pena imponible ¿cuál debería ser ese umbral mínimo? ¿Sería compatible con una previsión general de límite en tres años de prisión?

La Directiva sobre la privacidad y las comunicaciones electrónicas[2] establece que los Estados miembros pueden limitar los derechos de los ciudadanos cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional, la defensa y la seguridad pública, o garantizar la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas.

El Pronunciamiento que aquí comentamos es muy relevante, por cuanto las cuestiones planteadas por el órgano instructor español no son baladí, habida cuenta del parco marco normativo con el que cuenta, de ahí que la doctrina jurisprudencial, rica en un lenguaje poroso, voluble y lábil sea tan relevante para la delimitación del *iter* conceptual del contenido y alcance del derecho al secreto de las comunicaciones, "un clásico derecho de libertad-autonomía"[3], por cuanto es más abierto a la adecuación con la realidad social.

Para una parte de la doctrina consolidada, este derecho operaba como un "límite infranqueable"[4], salvo autorización judicial, pero esta Sentencia demuestra que, ante la tesitura entre seguridad y libertad, el criterio está cambiando. Si hasta ahora el TJUE había dado pasos firmes en la ponderación de las "circunstancias concurrentes para evitar

[1] Este mecanismo permite que los tribunales de los EE.MM., en el contexto de un litigio del que estén conociendo, interroguen al TJUE acerca de la interpretación del Derecho de la UE o sobre la validez de un acto de la Unión. El TJUE no resuelve el litigio nacional, y es el tribunal nacional quien debe resolver el litigio de conformidad con la decisión del TJUE.

[2] 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 (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).

[3] ARAGÓN, 2011, p. 190.

[4] COSTAS, 2018, p. 18.

un predominio indebido de una u otra que pueda desembocar en una injusticia"[5], como se desprende de la tesis mantenida con ocasión de los pronunciamientos contenidos en los casos *Tele2 Sverige* y *Watson*, en la Sentencia objeto de análisis exhibe una actitud hipergarantista y es el bien jurídico seguridad, como tendremos ocasión de ver, el bien jurídico que resulta reforzado.

2. BREVE EXÉGESIS DE LA RESOLUCIÓN: CUESTIONES PROCESALES Y SUSTANTIVAS

2.1. Sobre las cuestiones de carácter procesal

El *iter* procesal del presente Pronunciamiento, una Decisión de la Gran Sala, órgano colegiado compuesto por quince jueces cuya actuación está prevista *ex* artículo 16 del Estatuto del TJUE "cuando lo solicite un Estado miembro o una institución de la Unión que sea parte en el proceso" comienza con la admisión a trámite del auto remitido por el juez español.

El Alto Tribunal europeo avala *ab initio* su admisión a trámite. Así lo justifica en el Apdo. 46 de la Sentencia:

"En el presente asunto, el auto de remisión contiene los elementos de hecho y de Derecho suficientes tanto para la identificación de las disposiciones del Derecho de la Unión mencionadas en las cuestiones prejudiciales como para entender el alcance de estas cuestiones. En particular, del auto de remisión se desprende que las cuestiones prejudiciales planteadas tienen por objeto permitir al tribunal remitente apreciar si la norma nacional en la que se basa la solicitud de la Policía Judicial controvertida en el litigio principal persigue un objetivo que puede justificar una injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, y en qué medida. Pues bien, según ese mismo tribunal, dicha norma nacional está comprendida en el ámbito de aplicación de la Directiva 2002/58, de modo que la Carta resulta aplicable en el litigio principal. Así, las cuestiones prejudiciales guardan una relación directa con el objeto del litigio principal y, por tanto, no pueden considerarse hipotéticas".

2.2. Sobre las cuestiones de índole sustantiva

El Tribunal entra a examinar de forma conjunta las dos preguntas formuladas por el juzgador español. Al respecto, el Alto Tribunal europeo sostiene que:

"En cuanto a la existencia de una injerencia en los derechos fundamentales, procede recordar que, como señaló el Abogado General en los puntos 76 y 77 de sus conclusiones, el acceso de las autoridades públicas a estos datos constituye una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el artículo 7 de la Carta, incluso a falta de circunstancias que permitan calificar esta injerencia de ´grave` y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el artículo 8 de la Carta, puesto que constituye un tratamiento de datos personales [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU: C: 2017:592, apartados 124 y 126 y jurisprudencia citada]". (Apdo. 51)

El Alto Tribunal recoge en la *ratio decidendi* de esta Sentencia doctrina anterior que a su vez acoge las excepciones al principio de confidencialidad, que se sustentan en el precepto 15, apdo. 1, de la Directiva 2002/58. Recuerda el tribunal en esta ocasión que el catálogo de objetivos que pueden justificar este quiebro tiene un carácter exhaustivo:

"Por lo que respecta a los objetivos que pueden justificar una norma nacional, como la controvertida en el litigio principal, que regula el acceso de las autoridades públicas a los

[5] BANACLOCHE *et al.*, 2011, p. 167.

datos conservados por los proveedores de servicios de comunicaciones electrónicas y, por tanto, establece una excepción al principio de confidencialidad de las comunicaciones electrónicas, cabe recordar que la enumeración de los objetivos que figuran en el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 tiene carácter exhaustivo, de modo que dicho acceso ha de responder efectiva y estrictamente a uno de ellos (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartados 90 y 115)". (Apdo. 52)

Sin embargo, en pronunciamientos anteriores (por todos, *Tele2 Sverige* y *Watson*) a la calificación de exhaustividad, en una interpretación que abogada sin ambages por interpretar el precepto como un *numerus clausus*, la injerencia que supone el acceso a datos personales era posible en el marco de delito graves. Ahora, sin embargo:

"[…] puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general, al que se refiere el artículo 15, apartado 1, primera frase, de la Directiva 2002/58, sin que sea necesario que dichos delitos estén calificados como «graves»" (Apdo. 62)

A esta conclusión, que matiza sus tesis anteriores, llega tras alambrar esta cuestión en los apartados 53 a 57, el núcleo de la *ratio decidendi* de la presente Resolución. En particular:

"[…] el Tribunal de Justicia ha motivado esa interpretación basándose en que el objetivo perseguido por una norma que regula este acceso debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión que supone la operación (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartado 115)". (Apdo. 55)

Tanto a las cuestiones sobre el sentido de la norma y el umbral de los delitos responde el TJUE en el Apdo. 63, que cierra la fundamentación jurídica contenida en esta Decisión:

"Habida cuenta de las consideraciones anteriores, procede responder a las cuestiones prejudiciales planteadas que el artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7 y 8 de la Carta, debe interpretarse en el sentido de que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, consagrados en los citados artículos de la Carta, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.[…]".

A tenor de lo expuesto, para el Órgano jurisdiccional europeo el precepto 15 de la Directiva sobre la privacidad y las comunicaciones electrónicas, a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares (y su *corolario*) de las tarjetas SIM activadas con un teléfono móvil sustraído, constituye una injerencia en los derechos fundamentales de éstos, consagrados en los citados artículos de la Carta de los Derechos Fundamentales, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

3. CONCLUSIONES

El principio de proporcionalidad, influencia de la doctrina del Tribunal Constitucional alemán, es consustancial a los pronunciamientos del TJUE sobre la concreta cuestión del acceso a las comunicaciones y la posible afectación de los derechos fundamentales.

Este principio rector ha permeado en los órganos jurisdiccionales nacionales y ha cristalizado en la interiorización de la aplicación de un presupuesto triple -de legalidad, material y justificación teleológica-.

Al estar ayuno este sector normativo de la proporcionalidad, este presupuesto -de configuración jurisprudencial-, va a operar como un criterio determinante para enjuiciar la restricción de derechos fundamentales en los procesos penales.

Por ejemplo, en España, con un marco legal parco e insuficiente, los concretos requisitos del principio de proporcionalidad -idoneidad, necesidad y proporcionalidad en sentido estricto- han operado como condiciones *sine qua non* para que el juez motivara la concesión o denegación de una medida restrictiva sobre derechos fundamentales.

Sin embargo, hasta ahora, todo se asentaba y justificaba en la gravedad de los delitos. En este sentido, si en ocasiones anteriores (por todas, *Tele2 Sverige* y *Watson*) la clásica dicotomía entre la seguridad y la libertad había basculado en favor de esta última, en la Sentencia presente el TJUE se decanta por la primera.

De esta Resolución se derivan importantes consecuencias jurídico-procesales y jurídico-sustantivas. Así, en relación a las primeras, a partir de su publicación en el Diario Oficial de la Unión Europea, todos los tribunales nacionales deben seguir este criterio. En relación a las segundas, al matizar la interpretación de una norma (en este caso, un precepto de una Directiva) éste se entenderá interpretado en el sentido que ha plasmado el TJUE en esta Resolución de Gran Sala. E, igualmente, opera a partir su publicación en el Instrumento precitado.

REFERENCIAS

Aragón Reyes, M. *Derechos fundamentales y su protección*. Pamplona: Ed. Civitas. Madrid, 2011

Banacloche Palau, J. *Aspectos fundamentales de derecho procesal penal*. Madrid: Ed. La Ley. Madrid, 2011

Costas Rodal, L. *Intimidad, grabación de imagen y sonido y prueba en el proceso*. Pamplona: Ed. Aranzadi. Madrid, 2018