IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE[1]

Susanna Oromí i Vall-llovera
Universitat de Girona

Fecha de presentación: junio de 2019
Fecha de aceptación: marzo de 2020
Fecha de publicación: abril de 2020

Resumen

El Tribunal de Justicia de la UE reconoce que el acceso, la conservación y cesión de datos personales electrónicos, una de las diligencias de instrucción cada vez más utilizada en el proceso penal, constituye una injerencia en los derechos fundamentales a la vida privada y familiar y a la protección de datos de carácter personal, de forma que si una autoridad pública pretende obtener tales datos precisa de una autorización judicial que debe respetar en todo caso el principio de proporcionalidad y establece, como criterio de apreciación de la proporcionalidad, la gravedad de los delitos. Parece, pues, que el acceso a datos personales electrónicos en la investigación penal deberá limitarse estrictamente a fines de prevención y detección de delitos graves o el enjuiciamiento de tales delitos. De ahí surge la duda que se pretende resolver en este trabajo: ¿el juez de instrucción únicamente puede autorizar la obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones cuando se estén investigando delitos graves?; o, en una investigación penal, ¿cabe autorizar una diligencia de obtención y acceso a datos personales electrónicos cuando el delito no es grave? El TJUE ha dado recientemente una respuesta que es preciso analizar, pues sirve para fijar importantes criterios que debe utilizar el juez de instrucción en el juicio de proporcionalidad que fundamenta la autorización de este tipo de diligencias de instrucción.

Palabras clave

datos personales electrónicos, protección de datos de carácter personal, vida privada, diligencias de instrucción, investigación penal

1. Este trabajo se ha realizado en el marco del Proyecto de I+D (DER2017-82146-P).

Access to personal data held by electronic communications service providers in criminal investigations according to the Court of Justice of the EU[1].

Abstract

The EU Court of Justice recognises that accessing, holding and transferring electronic personal data, pretrial proceedings which are becoming more and more commonly used in criminal proceedings, constitutes interference in the fundamental rights to private and family life and to personal data protection, and therefore if a public authority attempts to obtain such data, it requires judicial authorisation which must in all cases respect the principle of proportionality and establishes, as a criterion of the evaluation of proportionality, the seriousness of the crimes. It seems, then, that access to electronic personal data in criminal investigation must be strictly limited to the purposes of prevention and the detection of serious crimes, or the trial of such crimes. This leads to the doubt which we attempt to resolve in this work: Can only the examining judge authorise obtaining electronic personal data held by communications service providers when serious crimes are being investigated? Or, in a criminal investigation, should proceedings for obtaining evidence and access to electronic personal data be authorised when the crime is not serious? The CJEU recently gave a response which requires analysis, as it serves to set important criteria that the examining judge must use in the judgement of proportionality which gives the foundation for the authorisation of these kinds of criminal pretrial proceedings.

Keywords

electronic personal data, personal data protection, private life, criminal pre-trial proceedings, criminal investigation

1. This work was carried out within the framework of the R+D Project (DER2017-82146-P).

1. Introducción

Uno de los medios de investigación cada vez más utilizados en la fase de instrucción de los procesos penales, tanto si se persigue la presunta comisión de delitos graves como de los que no revisten tal gravedad, es el acceso y obtención de datos de tráfico y localización de las comunicaciones electrónicas, en especial las que derivan de la telefonía móvil o internet. Tales datos tienen la consideración de datos personales de los ciudadanos y quedan amparados por el derecho a la protección de datos de carácter personal[2], por lo que se precisa autorización judicial para obtenerlos (artículo 588 *ter j* LE-Crim). El uso generalizado de la telefonía móvil en la sociedad ha propiciado que estas diligencias sumariales se hayan convertido en uno de los instrumentos más importantes de que dispone la policía judicial, la fiscalía y los jueces para perseguir la criminalidad. Lo habitual es que sea la policía judicial la que solicite al juez instructor tal diligencia de obtención y cesión de datos personales, siendo una de las medidas de investigación usada con mayor asiduidad en los últimos tiempos.

El Tribunal de Justicia de la UE (en adelante, TJUE) reconoce que la conservación y cesión de datos personales de tráfico constituye una injerencia en los derechos a la vida privada y familiar y a la protección de datos de carácter personal , garantizados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, la Carta), de forma que si una autoridad pública pretende obtener tales datos debe respetar en todo caso el principio de proporcionalidad y establecer, como criterio de apreciación de la proporcionalidad, la gravedad de los delitos como justificación de la obtención y cesión de los datos para las investigaciones penales[3]. Parece, pues, que el acceso de las autoridades competentes a los datos y su utilización ulterior en un proceso penal deberán limitarse estrictamente a fines de prevención y detección de delitos graves o el enjuiciamiento de tales delitos.

De ahí surge la duda que se pretende resolver en este trabajo: ¿el juez de instrucción únicamente puede autorizar la obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones cuando se estén investigando delitos graves?; o, en una investigación penal, ¿cabe autorizar una diligencia de obtención y cesión de datos personales electrónicos cuando el delito no es grave?

El TJUE ha dado recientemente una respuesta que es preciso analizar, pues sirve para fijar importantes criterios que deben utilizar los juzgados de instrucción en el juicio de proporcionalidad que fundamenta la autorización de este tipo de diligencias de instrucción[4]. Es otra muestra de cómo el uso de la tecnología en la sociedad –y de forma extensiva en la criminalidad– incide en la eficacia y la eficiencia de los procesos judiciales.

2. Por lo que se deben respetar las previsiones de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
3. STJUE de 8 de abril de 2014, *Digital Rights Ireland* y otros (C 293/12 y C 594/12, EU:C:2014:238), declaró la invalidez de la 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 comunicación, donde afirma: «Además, en cuanto al acceso de las autoridades nacionales competentes a los datos y su utilización posterior, la Directiva 2006/24 no precisa las condiciones materiales y de procedimiento correspondientes. El artículo 4 de la Directiva, que regula el acceso de dichas autoridades a los datos conservados, no dispone expresamente que el acceso y la utilización posterior de los datos de que se trata deberán limitarse estrictamente a fines de prevención y detección de delitos graves delimitados de forma precisa o al enjuiciamiento de tales delitos, sino que se limita a establecer que cada Estado miembro definirá el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad».
4. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), que tiene por objeto una petición de decisión prejudicial planteada por la Audiencia Provincial de Tarragona.

2. Injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal

Como se ha apuntado, el acceso por parte de autoridades públicas a datos personales de tráfico y localización de las comunicaciones electrónicas representa una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de datos personales, garantizados en los artículos 7 y 8 de la Carta. Así lo ha reiterado el TJUE en varias ocasiones, según se examina a continuación.

La injerencia en estos derechos fundamentales puede producirse a través de la comunicación, acceso y conservación de datos de carácter personal con vistas a su utilización por parte de las autoridades públicas o cualquier otra persona. Y esta injerencia se produce cualquiera que sea el uso posterior de la información comunicada o conservada. En este sentido, la injerencia en el derecho fundamental al respeto de la vida privada y familiar, consagrado en el artículo 7 de la Carta, se ocasiona con independencia de que la información sobre la vida privada tenga o no carácter sensible y sin que sea relevante que los interesados hayan padecido algún perjuicio o inconveniente. No es necesario, por tanto, que se trate de una injerencia grave en la vida privada de los ciudadanos, sino que cualquier tipo de acceso a datos personales electrónicos produce la vulneración del derecho fundamental[5].

Es más, tal comunicación, conservación y accesos a datos personales conservados por proveedores de servicios de comunicaciones electrónicas, sea cual sea su utilización posterior, también constituyen tratamientos de datos de carácter personal, por lo que configuran asimismo una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta[6].

Ni que decir tiene que, si el acceso de datos personales conservados por proveedores de servicios de comunicaciones electrónicas supone una injerencia en los derechos fundamentales a la vida privada y a la protección de datos de carácter personal, representa, a mi juicio, una vulneración de tales derechos; por tanto, cuando una autoridad pública pretenda acceder a estos datos, justificándolo en actuaciones de investigación de delitos, precisará en todo caso autorización judicial, y en el caso de que se practique la diligencia sin esta autorización cabrá alegar la ilicitud de la prueba en juicio oral.

Sentada, pues, la injerencia en los derechos fundamentales, procede examinar cuándo las autoridades públicas pueden acceder a datos personales electrónicos justificándolo en el desarrollo de investigaciones penales.

3. Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales por delitos graves

A la luz de todo lo expuesto, no hay ninguna duda que el acceso y obtención por autoridades policiales o judiciales, en el marco de investigaciones penales, de datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, representan una injerencia en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta. Pero esta excepción al principio de confidencialidad de las comunicaciones electrónicas se encuentra amparada por el artículo 15.1 de la Directiva 2002/58, que establece de forma exhaustiva los objetivos que permiten el acceso de autoridades públicas a tales datos, entre los que se encuentra «la prevención, investigación, descubrimiento y persecución de delitos». Cabe recordar que el TJUE ha reconocido que cualquier limitación a la confiden-

5. En relación con el artículo 7 de la Carta, lo viene señalando el TJUE en las siguientes sentencias: de 20 de mayo de 2003, Österreichischer Rundfunk y otros (C-465/00, C-138/01 y C-139/01, EU:C:2003:294), apartados 74 y 75; de 8 de abril de 2014, Digital Rights Ireland y otros (C 293/12 y C 594/12, EU:C:2014:238), apartados 33 a 35; de 6 de octubre de 2015, Schrems (C 362/14, EU:C:2015:650), apartado 87; y, de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 51.
6. Véanse, en este sentido, las sentencias del TJUE de 17 de octubre de 2013, Schwarz (C 291/12, EU:C:2013:670), apartado 25; de 8 de abril de 2014, Digital Rights Ireland y otros (C 293/12 y C 594/12, EU:C:2014:238), apartado 36; y, de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 51.

cialidad de las comunicaciones electrónicas y de los datos de tráfico relativos a ellas debe interpretarse en sentido estricto, de forma que la conservación de datos de tráfico y de localización solo debe realizarse durante un plazo limitado y justificado, por lo que no es posible articular un sistema de conservación y cesión generalizada e indiscriminada de estos datos[7]. Sentada esta premisa, al establecer la investigación criminal como un motivo que justifica el acceso y obtención de datos personales, han surgido dudas, en particular sobre si los delitos deben revestir un cierto nivel de gravedad para permitir la injerencia en los derechos fundamentales, que han llevado a recientes pronunciamientos del TJUE al respecto, los cuales son objeto de análisis en el presente trabajo.

En este sentido, T. Armenta Deu (2018, pág. 70); I. Colomer Hernández (2018, págs.77-78); J. Delgado Martín (2019); E. Frías Martínez (2019); Mª. I. Gónzalez Cano (2019, págs. 1.331 y sigs.); A. E. Gudín Rodríguez-Magariños (2017); M. Richard González (2018, págs. 475 y sigs.); y A. Sánchez Rubio (2018, págs. 506 y sigs.).

El TJUE ha declarado que cuando el acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas comporta una injerencia grave a los mencionados derechos fundamentales, tal injerencia únicamente puede autorizarse para luchar contra la delincuencia grave[8]. Esto hace que el juez de instrucción, en el momento de dictar su resolución motivada para autorizar esta diligencia, deba realizar un juicio de proporcionalidad entre, por un lado, la gravedad de la injerencia en los derechos fundamentales, con lo que tendrá que tener en cuenta la naturaleza de los datos que se quieren obtener, y, por otro lado, la gravedad de los hechos delictivos. Así las cosas, solo cuando los delitos son graves debe admitirse el acceso a datos electrónicos de carácter personal que provoquen una injerencia grave en los derechos a la vida privada y familiar y a la protección de datos personales.

Llegados a este punto, surge la necesidad de analizar los dos extremos necesarios para realizar el juicio de proporcionalidad: en primer lugar, qué criterios deben utilizarse para valorar que la injerencia en los derechos fundamentales es grave; y, en segundo lugar, cuándo un delito tendrá la consideración de grave. La importancia de saber estos extremos radica en que un juez de instrucción únicamente podrá autorizar el acceso a datos personales si puede motivar este juicio de proporcionalidad.

3.1. ¿Qué criterios deben utilizarse para valorar que una injerencia en los derechos fundamentales a la vida priva y familiar y a la protección de datos de carácter personal es grave?

El TJUE ha interpretado que cuando una norma regula el acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, en materia de prevención, descubrimiento, investigación y persecución de delitos, debe guardar relación con la gravedad de la injerencia de los derechos fundamentales en cuestión[9], de forma que solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia también considerada como grave. De ahí que surja el interés por determinar qué se entiende por injerencia grave en los derechos fundamentales a la vida privada y familiar y a la protección de datos de carácter personal.

Una injerencia grave en los derechos fundamentales mencionados es aquella que permite extraer conclusiones precisas y concretas sobre la vida privada de las personas, cuyos datos han sido conservados por los proveedores de servicios de comunicaciones electrónicas. Así lo ha venido entendiendo el TJUE en varias de sus sentencias[10]. Por lo tanto, tienen la consideración de injerencia grave: acceder a las comunicaciones efectuadas con un teléfono móvil; conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas; obtener los lugares en que

7. STJUE de 22 de noviembre de 2012, Probst (C-119/12, EU:C:2012:748), apartado 23. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970).
8. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartado 99. STJUE de 8 de abril de 2014, Digital Rights Ireland y otros (C 293/12 y C 594/12, EU:C:2014:238). STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 56.
9. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartado 115.
10. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartado 99. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 56.

estas comunicaciones tuvieron lugar o la localización del terminal; o, saber la frecuencia de estas comunicaciones con determinadas personas durante un período concreto[11]. Todas estas actuaciones permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados, constituyendo una injerencia grave en los derechos a la vida privada y familiar y a la protección de datos de carácter personal.

Una injerencia de estas características únicamente queda justificada si se persigue la prevención, el descubrimiento, la persecución o la investigación de delitos graves. Por lo que es importante determinar también cuándo un delito tiene la consideración de grave, como se verá en el siguiente apartado.

3.2. ¿Cuándo un delito tiene la consideración de grave?

El TJUE no se pronuncia sobre este extremo de forma expresa, pese a la pregunta formulada en cuestión prejudicial por la Audiencia Provincial de Tarragona[12]. La STJUE (Gran Sala), de 21 de diciembre de 2016, tampoco recoge una definición cerrada de «delincuencia grave» y se limita a relacionarla con la delincuencia organizada y el terrorismo[13]. A nadie escapa que existen otras conductas delictivas consideradas como graves.

La duda planteada es procedente, pues cabe preguntarse si para considerar la gravedad de un delito únicamente debe tenerse en cuenta la pena que pueda imponerse o deben valorarse particulares niveles de lesividad en la conducta delictiva sobre determinados bienes jurídicos o el perjuicio causado a las víctimas; y, en el caso de que se opte por solo utilizar el criterio de la gravedad de la pena, entendiendo que la pena de prisión es la más grave que cabe imponer, ¿cuántos años de prisión como mínimo deben poder imponerse para considerar que el delito es grave?

La cuestión no es baladí en el sistema penal español, pues la legislación aplicable puede inducir a diferentes interpretaciones. Según el artículo 33.2 del Código Penal, son penas graves la prisión permanente revisable y la prisión superior a cinco años, entre otras. Pero conforme al artículo 588 *ter a* de la LECrim, que se remite al 579.1 del mismo texto legal, para precisar los delitos que pueden investigarse con este tipo de diligencias, fija el umbral mínimo de tres años de prisión. Una parte de la doctrina, que considero más razonable, entiende que, para fijar la gravedad de un delito en materia de cesión de datos, también deben utilizarse otros criterios como las circunstancias concretas de la conducta delictiva y el perjuicio causado a las víctimas[14].

El TJUE, empero, entiende que la mencionada cuestión prejudicial planteada por la Audiencia Provincial de Tarragona tiene por objeto apreciar si la norma nacional en la que se basa la solicitud de la policía judicial persigue un objetivo que puede justificar una injerencia en los derechos fundamentales a la vida priva y familiar y a la protección de datos de carácter personal[15], y no entra en determinar qué debe entenderse por delincuencia grave como criterio ponderativo. Parece pues que deja a la normativa y jurisprudencia interna de los Estados miembros la determinación de esta cuestión.

11. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 60.
12. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 26: «1) ¿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?; 2) En su caso, 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, EU:C:2014:238] 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?».
13. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartado 103.
14. J. L. Rodríguez Lainz (2012); L. Vázquez Seco (2017, págs. 19-24); J. Ortiz Pradillo (2017); y M. Bahamonde Blanco (2018); J. Pérez Gil (2019). La misma problemática la plantea M. Marchena Gómez (2014) en la ponencia presentada en el Observatorio de Derecho Penal Económico 2014.
15. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 49: «la petición de decisión prejudicial no tiene por objeto determinar si los datos personales de que se trata en el litigio principal han sido conservados por los proveedores de servicios de comunicaciones electrónicas de conformidad con los requisitos establecidos en el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7 y 8 de la Carta». En este sentido, J. L. Rodríguez Lainz (2018).

Así las cosas, sin perjuicio de que también deberían tenerse en cuenta otras circunstancias, delito grave en el sistema penal español es el que impone una pena grave, que según el artículo 33.2 del Código Penal es la de prisión superior a cinco años. Por tanto, los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión e inferior a cinco años de prisión, cuya investigación también admite una diligencia de acceso y obtención de datos personales obrantes en archivos automatizados de los prestadores de servicios, no tiene la consideración de delito grave, pues están castigados con penas menos graves según el artículo 33.3 del Código Penal. En consecuencia, parece, a simple vista, que si se investigan estos últimos delitos no se debe autorizar la diligencia de investigación, al no estar fundada esta en un tipo de delincuencia considerada grave[16]. De ahí surge la siguiente pregunta.

3.3. ¿El juez de instrucción únicamente puede autorizar la obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones cuando se estén investigando delitos graves?

De lo expuesto hasta este momento, se podría concluir que la única posibilidad que tiene un juez de instrucción para autorizar esta diligencia es cuando la obtención de los datos personales electrónicos represente una injerencia grave en los derechos fundamentales y se encuentre justificada por la gravedad del hecho delictivo. Esto es lo mismo que decir que siempre que el delito sea considerado grave el juez de instrucción debe autorizar esta diligencia de obtención de datos personales, con independencia de que la injerencia en los derechos fundamentales sea grave o no. Nadie puede poner en duda esta premisa, pues así debe acordarlo el juez en todo caso. Cabe preguntarse, empero, por qué es importante saber cuándo una obtención de datos representa una injerencia grave en los derechos fundamentales, pues parece que lo transcendente a tales efectos es fijar la gravedad del delito. La importancia surge, como se tendrá ocasión de comprobar en el siguiente apartado, cuando se solicita esta diligencia sumarial en procesos penales en los que se persiguen delitos que no son graves, casos muy habituales y donde se precisan tales diligencias de investigación por el amplio uso de la telefonía móvil y de la tecnología en la sociedad. Esto provoca que presuntos hechos delictivos no puedan llegar a ser esclarecidos dado que la única diligencia posible para acreditarlos es la obtención de datos electrónicos conservados por prestadores de servicios.

La respuesta a la pregunta planteada es obviamente negativa. El juez de instrucción puede autorizar la obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones electrónicas en los procesos que se estén investigando delitos graves, motivándolo en la lucha contra la delincuencia grave. Ahora bien, no puede hacerlo únicamente en estos procesos penales por delitos graves, pues cuando se persiguen delitos que no son graves, si concurren los criterios que analizaremos a continuación, también puede autorizar este tipo de diligencias de investigación.

4. Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales por delitos no graves

Ha quedado claro, de lo expuesto hasta este momento, que una injerencia grave en los derechos fundamentales previstos en los artículos 7 y 8 de la Carta, causada por una solicitud policial o de fiscalía de acceso y obtención de datos personales conservados por prestadores de servicios de comunicaciones electrónicas, solo puede justificarse en la persecución, investigación o descubrimientos de delincuencia grave. Ahora bien, también es posible que esta clase de diligencias de investigación se

16. Esto es lo que sucedió en la investigación de un robo con violencia de un teléfono móvil que da origen a la cuestión prejudicial planteada por la Audiencia Provincial de Tarragona, resuelta por la STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788): ante la solicitud de la policía judicial de que se ordenase a determinados proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfono activados, desde el 16 de febrero hasta el 27 de febrero de 2015, con el código IMEI del teléfono móvil sustraído, así como el nombre, apellidos y dirección de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, el juez de instrucción denegó la diligencia considerando que esta cesión de datos se limita a los delitos graves, y los hechos presuntos del caso no eran constitutivos de tal tipo de delito.

soliciten en procesos penales por delitos no graves y cabe examinar si es posible su autorización, sin perder de vista, de entrada, que si esta solicitud comporta una injerencia grave en los derechos a la vida privada y familiar o a la protección de datos de carácter personal, el juez no la podrá autorizar, pues los hechos delictivos no revisten la gravedad suficiente para motivar la injerencia grave en los derechos fundamentales, de acuerdo con el principio de proporcionalidad. Pero ¿qué ocurre cuando la injerencia en los derechos fundamentales puede considerarse como no grave?

Cabe recordar, llegados a este punto, que una de las excepciones al principio de confidencialidad de las comunicaciones electrónicas, que permite el acceso de las autoridades públicas a los datos conservados por los proveedores de las comunicaciones electrónicas, establecidas con carácter exhaustivo en el artículo 15 de la Directiva 2002/58[17], se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos[18]. Pues bien, este artículo no limita el acceso de las autoridades públicas a datos de carácter personal en los supuestos de persecución de delitos graves, sino que lo permite cuando se trate de cualquier tipo de delito, sea grave o no lo sea[19].

De ahí que cuando la policía judicial solicita al juez de instrucción el acceso y obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones, si el contenido de esta solicitud puede ser calificado como una injerencia no grave de los derechos fundamentales a la vida privada y familiar y a la protección de datos de carácter personal, el juez puede autorizarlo, justificándolo en la prevención, investigación, descubrimiento y persecución de delitos, incluso cuando estos no sean graves. Así lo ha reconocido el TJUE: «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»[20].

En concreto, en un apartado anterior hemos señalado supuestos de acceso y obtención de datos de carácter personal conservados por proveedores de servicios de comunicaciones electrónicas, considerados por el TJUE como injerencias graves de los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta. En el mismo sentido, el TJUE indica casos en que tal solicitud de acceso y obtención de datos no tendrá la consideración de injerencia grave sino una mera injerencia en los derechos fundamentales: cuando se solicita identificar a los titulares de las tarjetas SIM activadas durante un determinado período de tiempo con el número IMEI de un concreto teléfono móvil, con objeto de tener los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y dirección.

Ahora bien, la jurisprudencia española ha entendido que este tipo de diligencias de identificación de SIM y número IMEI no implica obtener datos vinculados a un proceso de comunicación, por lo que no comportaría vulneración del derecho a la intimidad o al secreto de las comunicaciones, de forma que su autorización no precisa resolución judicial motivada, y así se ha establecido en el artículo 588 *ter m* LECrim[21]. Parece, por tanto, que existe una contradicción evidente entre la doctrina del TJUE, que considera este tipo de acceso a datos personales como una injerencia no grave de los derechos fundamentales a la protección de datos de carácter personal y a la vida privada y familiar, y el sistema español, lo que hace surgir la duda sobre si el artículo 588 *ter m* LE-Crim es conforme al derecho de la Unión Europea. A mi juicio, pese a que la injerencia no es grave, sigue siendo una vulneración de los derechos fundamentales de los ciudadanos que debe precisar de autorización judicial, pues motivos de eficiencia judicial,

17. «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). DOCE (31 de julio de 2002), L 201/37.
18. Sobre el carácter exhaustivo de tales objetivos, ver la STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartados 90 y 115.
19. Así lo ha interpretado el TJUE en su sentencia (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 53.
20. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 57.
21. STS (Sala de lo Penal, Sección 1.ª) núm. 492/2010 de 18 mayo (RJ 2010\5814); STS (Sala de lo Penal, Sección 1.ª), núm. 1344/2009 de 16 diciembre (RJ 2010\308), entre otras. Para un análisis en profundidad véase A. Peralta Gutiérrez y P. Aguirre Allende (2019). En cambio, J. L. Rodríguez Laiz (2019) considera que no se producen comunicaciones electrónicas cuando se obtiene información sobre la asociación entre terminal físico y tarjeta SIM.

esto es, el gran número de diligencias que deban autorizar los jueces provocando gran volumen de trabajo para los juzgados de instrucción, no puede justificar una injerencia en derechos fundamentales sin resolución judicial, aunque tenga la consideración de no grave.

Lo que se deja claro es que esta injerencia no grave en ningún caso puede comportar conocer las comunicaciones efectuadas con el teléfono móvil ni su localización, pues en este último caso estaríamos ante una injerencia grave de los derechos fundamentales mencionados, cuya autorización judicial solo cabe realizarse para la investigación o descubrimiento de delitos graves. En este sentido, toda petición de obtención de datos de carácter personal que no comporte «extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados»[22], puede autorizarse al representar una injerencia no grave en los derechos fundamentales de los artículos 7 y 8 de la Carta. Si estamos ante este tipo de injerencias no graves, el juez de instrucción puede autorizar motivadamente la diligencia de investigación solicitada, aunque el delito objeto de investigación no sea grave. Por tanto, la falta de gravedad del delito no puede justificar, por sí sola, la no autorización judicial de estas diligencias.

5. Conclusiones: juicio de proporcionalidad del juez de instrucción

Es preciso sentar, antes de incidir en la proporcionalidad que debe apreciar el juez, que cuando una autoridad pública, como la policía judicial o el fiscal, pretenda acceder a datos personales conservados por proveedores de servicios de comunicaciones electrónicas, justificándolo en la investigación de algún delito, precisará en todo caso de autorización judicial, por lo que, en caso de practicar tal diligencia sin la oportuna resolución judicial, la parte afectada podrá alegar la ilicitud de la prueba en juicio oral por obtención de prueba vulnerando derechos fundamentales.

Así las cosas, cabe concluir que lo importante para poder decidir si se debe autorizar el acceso y obtención de datos personales conservados por proveedores de servicios de comunicaciones electrónicas es el juicio de proporcionalidad que debe realizar el juez de instrucción, valorando, de un lado, la gravedad de la injerencia en los derechos fundamentales y, de otro, la gravedad de los hechos delictivos. Solo así se podrá tener en cuenta el nivel de afectación o injerencia en los derechos fundamentales relacionados con la protección de datos de carácter personal y con la vida privada y familiar en el ámbito de la confidencialidad de las comunicaciones.

En efecto, lo primero que debe hacer el juez es determinar si la diligencia concreta de acceso a datos personales electrónicos que solicita la policía judicial o la fiscalía, a efectos de la investigación de un delito, debe considerarse una injerencia grave en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, o si no reviste tal gravedad; y, una vez determinada la gravedad de la injerencia, es preciso fijar si la delincuencia objeto de investigación es grave o no. Debe realizar tal juicio de proporcionalidad, pues el juez de instrucción únicamente puede autorizar una diligencia de investigación que suponga una injerencia grave en los derechos fundamentales cuando los hechos objeto de investigación puedan tener la consideración de delito grave. Si se trata de un delito que no revista tal gravedad y la diligencia comporta una injerencia grave en los derechos fundamentales, no cabrá autorizar su práctica.

Así parece indicarlo el mismo artículo 588 *ter j* de la LECrim, cuando establece que la solicitud de la diligencia de investigación debe precisar «la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión», pues «la naturaleza de los datos» servirá para valorar la gravedad de la injerencia en los derechos fundamentales y «las razones de la cesión» determinará el nivel de gravedad de los hechos delictivos. Con estos extremos, el juez puede realizar el juicio de proporcionalidad para decidir si autoriza o no la diligencia de investigación.

Se observa que es importante valorar cuándo la injerencia en los derechos fundamentales no es grave o cuándo reviste una especial gravedad. El TJUE, como se ha tenido ocasión de comprobar, ha ido señalando supuestos concretos de injerencia grave y no grave. En este sentido, ha entendido que cuando se solicita identificar a los titulares de las tarjetas SIM

22. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartados 59, 60 y 62.

activadas durante un determinado período de tiempo con el número IMEI de un concreto teléfono móvil, con el objeto de tener los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y dirección, no se trata de una injerencia grave en los derechos fundamentales. En estos casos, el artículo 588 *ter m* LECRim no exige resolución judicial motivada para acceder a estos datos, cosa que parece contradictoria con la interpretación del TJUE y hace surgir dudas sobre si esta regulación es conforme con el derecho de la Unión Europea. Pese a que la injerencia en los derechos fundamentales no es grave, no deja de ser una injerencia, de forma que su práctica precisa autorización judicial, pues motivos de eficiencia judicial, como son el gran número de estas diligencias que deban autorizar los jueces, las cuales aumentarían su volumen de trabajo, no pueden justificar una injerencia en derechos fundamentales sin resolución judicial, aunque tenga la consideración de injerencia no grave.

En consecuencia, como se ha tenido ocasión de comprobar, cuando el juez entienda que la injerencia en los derechos fundamentales a la vida priva y familiar o a la protección de datos de carácter personal no es grave, puede autorizar la diligencia de acceso y obtención de datos con el objeto de prevenir, descubrir, investigar o perseguir delitos en general, sin necesidad de valorar la gravedad de los hechos delictivos; en cambio, cuando se trate de injerencias graves en los derechos a la vida privada y familiar y a la protección de datos de carácter personal, tal injerencia solo puede fundamentarse en la persecución, descubrimiento, prevención o investigación de delitos graves. Ahora bien, la falta de gravedad del delito no puede justificar, por sí sola, la no autorización judicial de una de estas diligencias de investigación.

Referencias bibliográficas

ARMENTA DEU, T. (2018). «Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre». *IDP. Revista de Internet, Derecho y Política,* núm. 27, págs. 67-79. https://doi.org/10.7238/idp.v0i27.3149

BAHAMONDE BLANCO, M. (2018). «Medidas de investigación tecnológica a la luz de los Derechos Fundamentales, una cuestión pendiente». *Diario La Ley*, núm. 9.160.

COLOMER HERNÁNDEZ, I. (2018). «La cesión de datos de las comunicaciones electrónicas para su uso en investigaciones criminales: una problemática en ciernes». En: F. JIMÉNEZ CONDE (dir.). *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales*. Valencia: Tirant lo Blanch, págs. 77 y sigs.

DELGADO MARTÍN, J. (2019). «Protección de datos y prueba en el proceso». *Diario La Ley,* núm. 9.383.

FRÍAS MARTÍNEZ, E. (2019). «Obtención de datos personales en procesos penales y administrativos». *Diario La Ley,* núm. 9.404.

GONZÁLEZ CANO, M.ª I. (2019). «Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680» [en línea]. *Revista Brasileira de Direito Processual Penal, Porto Alegre*, núm. 3(5), págs. 1.331-1.384. https://doi.org/10.22197/rbdpp.v5i3.279.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E. (2017). «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información». *La Ley Penal*, núm. 125.

MARCHENA GOMEZ, M. (2014). «El futuro de las diligencias probatorias relacionadas con las nuevas tecnologías de la información y la comunicación, a partir de los contenidos del Borrador de Código Procesal Penal» [en línea]. *Observatorio de Derecho Penal Económico 2014*. Madrid: Universidad Rey Juan Carlos- KPMG. http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUszEONTtbLUouLM_DxbIwNDEwNzQwuQQGZapUtckhIQaptWmJOcSoAPL5kezUAAAA=WKE [Fecha de consulta: 14 de marzo de 2020].

ORTIZ PRADILLO, J. (2017). «Comunicaciones, tecnología y proceso penal: viejos delitos, nuevas necesidades». En: J. M. ASENCIO MELLADO (dir.). *Justicia penal y nuevas formas de delincuencia.* Valencia: Tirant lo Blanch, págs. 23-28.

PERALTA GUTIÉRREZ, A.; AGUIRRE ALLENDE, P. (2019). «El TJUE y el acceso a los datos de abonado en el seno de la instrucción penal». *Diario La Ley*, núm. 9.420.

PÉREZ GIL, J. (2019). «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal». En: F. JIMÉNEZ CONDE; F. BELLIDO PENADÉS (dirs.). *Justicia: ¿garantías versus eficiencia?* Valencia: Tirant lo Blanch, págs. 399 y sigs.

RICHARD GONZÁLEZ, M. (2018). «La conservación y utilización de datos de las comunicaciones en la investigación criminal. Problemas que resultan de la aplicación de la doctrina del TJUE». En: F. JIMÉNEZ

CONDE (dir.). *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales.* Valencia: Tirant lo Blanch, págs. 475 y sigs.

RODRÍGUEZ LAINZ, J. L. (2012). «Hacia un nuevo entendimiento de gravedad del delito en la Ley de conservación de datos relativos a las comunicaciones electrónicas». *Diario La Ley*, núm. 7.789.

– (2018). «El régimen legal español en materia de conservación y cesión de datos para la investigación de delitos». *Diario La Ley,* núm. 9.291, Sección Doctrina.

SÁNCHEZ RUBIO, A. (2018). «La necesaria adecuación del derecho interno a la normativa europea sobre tratamiento de datos de las comunicaciones electrónicas en la investigación penal». En: F. JIMÉNEZ CONDE (dir.). Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales. Valencia: Tirant lo Blanch, págs. 506 y sigs.

VÁZQUEZ SECO, L. (2017). «Incorporación de datos al proceso. Vigencia de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a redes públicas e interpretación de la ley a la luz de la reforma operada por la LO 13/2015». Madrid: Centro de Estudios Jurídicos. Universidad Complutense de Madrid, págs. 19-24.

Cita recomendada

OROMÍ I VALL-LLOVERA, Susanna (2020). «Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE». IDP. Revista de Internet, Derecho y Política. N.º 31. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3206

Sobre la autora

Susanna Oromí i Vall-llovera
soromi@uoc.edu
Universitat de Girona

Licenciada en Derecho (1996) y doctora en Derecho (2000) por la Universitat de Girona. Ha sido becaria FI de la Generalitat de Catalunya y profesora ayudante, también en la Universitat de Girona. Ha realizado estancias de investigación predoctoral en el Institut für Bürgerliches Recht und Zivilprozeβrecht (Universidad de Múnich, Alemania) y posdoctoral en la Universidad Paris X-Nanterre. En la actualidad es profesora titular de Derecho Procesal y directora del Departamento de Derecho Público de la Universitat de Girona. Asimismo, forma parte del Grup de Recerca Consolidat de la Generalitat de Catalunya «Cuestiones actuales de Derecho Procesal», y centra su investigación en la Administración de Justicia y en los procesos civil y penal. Entre sus publicaciones destacan: El ejercicio de la acción popular o Intervención voluntaria de terceros en el proceso civil. Ha sido coordinadora científica del proyecto europeo financiado por la Comisión Europea (Action grant, sobre «The protection of the victims in the European criminal justice systems»), además de haber participado activamente, como IP o como miembro, en más de una decena de proyectos de investigación nacionales y europeos.

Universitat Oberta de Catalunya