InDret
4.2020

Diligencias de investigación, cesión de datos y principio de proporcionalidad

María Jesús Pesqueira Zamora
Universidad Abat Oliba

Sumario

El presente trabajo pretende abordar el análisis de una nueva medida de investigación, prevista en los arts. 579 y 588 ter j LECrim, por la que se autoriza la cesión de datos y archivos informáticos, como herramienta idónea para la lucha contra la delincuencia grave. El debate jurídico se origina con motivo de una cuestión prejudicial (STJUE asunto C-207/16, de 2 de octubre de 2018), en tanto en cuanto supone una vulneración de los arts. 7 y 8 de la CEDF, relativos al respeto a la vida privada y familiar. Como diligencia que comportará la intromisión del Estado en las comunicaciones telemáticas de las personas investigadas en procesos judiciales y, en atención a los derechos afectados, el concepto de proporcionalidad será utilizado como criterio adecuado para determinar la gradación en el nivel de injerencia de la medida. A falta de una regulación clara y específica, la jurisprudencia del TJUE marcará, por un lado, el sentido interpretativo del TJUE en esta materia, y por otro, evidenciará la necesidad de una efectiva armonización de las legislaciones europeas cuyos estándares de protección de los derechos fundamentales sean equivalentes.

Abstract

This work aims to address the analysis of a new research measure, envisaged in the arts 579 and 588 ter LECrim, authorizing the transfer of data and computer files, as an appropriate tool for the fight against serious crime. The legal debate arises on the occasion of a question referred for a preliminary ruling (Case STJUE C-207/16 of 2 October 2018), in so far as it constitutes an infringement of the arts. ECDF 7 and 8 concerning respect for private and family life. As a diligence involving state intrusion into the telematic communications of persons investigated in judicial proceedings and, in view of the rights concerned, the concept of proportionality will be used as an appropriate criterion for determining the level of interference of the measure. In the absence of clear and specific regulation, the case-law of the CJEC will mark, on the one hand, the interpretative meaning of the CJEC in this area and, on the other hand, demonstrate the need for effective harmonisation of European legislation whose rules for the protection of fundamental rights are equivalent.

Title: Criminal investigation proceedings, data transfer and principle of proportionality

Palabras clave: *Diligencias de investigación, Cesión de Datos, Principio de proporcionalidad, Protección Derechos Fundamentales, Jurisprudencia TJUE, Ley de Enjuiciamiento Criminal, Carta de Derechos Fundamentales de la Unión Europea*
Keywords: *Investigative Diligence, Data Transfer, Principle of Proportionality, Protection Fundamental Rights, CJEU Jurisprudence, Criminal Procedural Law, Charter Fundamental Rights of de European Union*

DOI: 10.31009/InDret.2020.i4.11

InDret

4.2020

Recepción
21/05/2020
-
Aceptación
09/09/2020
-

Índice

-

1. Introducción
2. Cesión de datos y archivos informáticos: concepto y características
3. Derechos afectados
4. Eficacia y garantía de la cesión de datos
5. Regulación
5.1. Aplicabilidad del Derecho nacional – Derecho europeo
5.2. Competencia del TJUE y protección de los Derechos Fundamentales
a. Consideraciones generales
b. Consideraciones particulares en la diligencia de cesión de datos
6. Fundamento jurídico de la medida en el ordenamiento de la UE
6.1. Construcción de una Europa de Libertad, Seguridad y Justicia
6.2. Principios de cooperación en materia penal, reconocimiento mutuo y confianza entre los Estados
6.3. Principio de disponibilidad de datos
7. La evolución del principio de proporcionalidad en torno a la cesión de datos a la luz de la jurisprudencia del TJUE
7.1. Principio de proporcionalidad en relación al principio de disponibilidad de datos
7.2. Principio de proporcionalidad en relación al principio de especialidad en el tratamiento de datos personales
7.3. Última "vuelta de tuerca" del principio de proporcionalidad en relación al tratamiento de datos personales en cuanto al alcance del delito grave
8. Conclusiones
9. Bibliografía

-

-

1. Introducción*

Desde un punto de vista sociológico, el progreso de la tecnología, y particularmente, de la Tecnología de la Información y Comunicación (TIC), conlleva la introducción de las nuevas tecnologías en la sociedad actual y comporta el aumento del uso de las mismas, ya sea en el número de usuarios o en el tiempo empleado en el consumo tecnológico.

La incursión de Internet, y en general, de los nuevos medios de comunicación, incrementa notoriamente el intercambio de información entre sus usuarios, a través de estos nuevos sistemas, configurando un mundo cada vez más virtual, cuya particularidad se concreta en la inmediatez y la facilidad de acceso, y rige, consecuentemente, un cambio en la manera de comunicarnos y adquirir nuevos conocimientos[1].

En la era digital en la que convergemos, ya no se comprenden las relaciones entre sujetos sin la intervención de la tecnología y sus medios digitales. Así, en la sociedad de la información del siglo XXI, las nuevas tecnologías se emplean no únicamente como mecanismo de propagación de la información, sino que se distinguen por ser un medio de interacción y confluencia entre personas que poseen unos idénticos o dispares intereses e ideas.

La proliferación y el desarrollo geométrico de las nuevas tecnologías es patente en nuestro quehacer habitual, y se revela en el constante intercambio de información personal o laboral o de cualquier tipo evidenciando una cesión de datos que pertenecen a la más estricta intimidad de cada persona, y autorizando tácitamente a que éstos queden sometidos al control virtual por parte de los demás usuarios, así como también, de las empresas que administran las citadas redes sociales. Se desprende pues, que su uso se ha convertido en el principal instrumento de trabajo, de ocio y esencialmente de relación social entre las personas. Lamentablemente, no podemos obviar que la tecnología se hace extensiva a nuevas formas delictivas que a su vez requerirán instrumentos idóneos para la investigación y prevención de esos delitos[2].

En este sentido, el sistema judicial debe dar respuesta y adecuarse a la nueva realidad tecnológica que se proyecta, comprometiéndose con los retos que se desprenden de la sociedad de la información, amparando los cambios sociales actuales vinculados con el intercambio de datos a través de redes de comunicación.

Las novedades en las que se fundamentan las nuevas tecnologías, constituyen una nueva realidad para el derecho, que debe adaptarse vertiginosamente a los desafíos diarios que estas presentan, pues el progreso tecnológico es más acelerado que la propuesta normativa del legislador.

---

* Correo electrónico de la autora: mpesqueiraz@uao.es

[1] La relevancia actual en la crisis del Coronavirus y la paralela preocupación de la UE por el control de los datos puede derivar en una vulneración sistemática del derecho a la privacidad de todas las personas (https://www.aepd.es/es/prensa-y-comunicacion/blog/notificacion-de-brechas-de-seguridad-de-los-datos-personales-durante-el; https://www.economistjurist.es/actualidad-juridica/el-gobierno-aprueba-la-geolocalizacion-en-el-estado-de-alarma/

[2] Fernando GASCÓN INCHAUSTI (2012), *Investigación transfronteriza, obtención de prueba penal en el extranjero y derechos fundamentales* (Reflexiones a la luz de la jurisprudencia español), Derecho Procesal Español del S. XX a golpe de tango, Tirant lo Blanch, p. 1254.

Es preciso, por lo tanto, que el derecho y las nuevas tecnologías progresen y se perfeccionen de manera paralela, con el fin de dar respuesta a las nuevas realidades que se presentan.

En el plano normativo es loable el esfuerzo realizado por el legislador-tantas veces reivindicado por la jurisprudencia[3] y la doctrina[4]-al regular una amplia lista de diligencias que implicarán una mejora en la eficacia de los procesos judiciales para la averiguación de hechos delictivos[5]. Sin embargo, cada una de las medidas contempladas exige su adecuación al caso concreto, mediante la aplicación de los principios procesales que más tarde abordaremos, así como de la interpretación jurisprudencial que irá precisando su correcta adopción.

En este trabajo analizaremos la medida prevista en el art. 588 ter j LECrim mediante la cual el juez de instrucción podrá autorizar la cesión de los datos electrónicos conservados por los prestadores de servicios de telecomunicaciones que revelan la procedencia e identidad de los interlocutores u otro dato de tráfico anexo al proceso, para la averiguación de informaciones que permitan avanzar en la prevención y persecución de la delincuencia. Una vez los datos de comunicación han sido intervenidos y depositados, se integran en unos registros cuya conservación viene a ser preceptiva para los distintos operadores informáticos. Por este motivo debemos examinar las garantías ofrecidas para que dicha custodia no incida indebidamente en los derechos fundamentales de las personas afectadas por la medida.

Atendiendo al riesgo que plantea la diligencia, esta medida está prevista únicamente para delitos graves de conformidad con el art. 579, 1º LECrim. En consecuencia, es necesario identificar el elemento a tener en cuenta para llegar a calificar un delito como grave: o bien la pena que lleva aparejada o bien la especial lesividad de las conductas delictivas[6].
En este horizonte, resulta determinante el alcance del principio de proporcionalidad, parámetro general, en relación al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones, a la luz de la última resolución del TJUE[7] completando así, estudios

[3] STC 145/2014, de 22 de septiembre.

[4] Raquel CASTILLEJO MANZANARES (2010) *Hacia un nuevo proceso penal*, La Ley, Madrid. Julio BANACLOCHE PALAO. y Jesús ZARZALEJOS NIETO (2015), *Aspectos fundamentales del Derecho procesal penal*, La Ley, Madrid.

[5] Con ello se cumple con las obligaciones impuestas con motivo de la ratificación del Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001. Dicho esfuerzo llega a tiempo de remediar importantes vacíos. Véase al respecto Gemma GALLEGO SÁNCHEZ (2010), *Sobre el secreto de las comunicaciones*, el art. 579 LECrim y las intervenciones telefónicas». *El Derecho. com,* <http://www.elderecho.com/tribuna/penal/secreto-comunicaciones-LECrim-intervenciones-telefonicas_11_159055012.html>. Pero con toda probabilidad precisará de importantes adecuaciones ante la velocidad con que se desarrollan los acontecimientos y estas técnicas, lamentablemente siempre por delante de la correspondiente protección de los ciudadanos.

[6] Cuestión prejudicial C-207/16 de la Audiencia Provincial de Tarragona, suscitada con motivo de la denegación de la autorización para que la policía judicial accediera a la información de un dispositivo previamente sustraído durante la tramitación de una causa de robo con violencia, por considerar el titular del órgano judicial que dicha medida podría resultar desproporcionada en cuanto a la intromisión del derecho a la intimidad de los sujetos investigados.

[7] Asimismo, existen estudios previos que realizan un análisis pormenorizado de la medida pero resultan incompletos al haberse dictado una resolución posterior en relación al mismo

previos ya publicados[8]. En una materia tan "viva" recabar toda la jurisprudencia actualizada al respecto resulta inexcusable. Este será el objeto fundamental de nuestro análisis.

2. Cesión de datos y archivos informáticos: concepto y características

En un proceso comunicativo (telefónico o telemático) podemos diferenciar entre su contenido y los datos de tráfico del mismo, esto es, aquella información de identificación de los medios de comunicación emisores y receptores que se genera como consecuencia de conducción de una comunicación[9].

Conviene advertir que la doctrina[10] ha clasificado los medios de investigación tecnológica en dos fuentes de prueba:

a) La primera fuente de prueba se refiere a los procesos comunicativos. En concreto, las previsiones legales establecidas son la intervención de las comunicaciones sostenida a través de tecnologías de la información, la interceptación de comunicaciones personales efectuadas a través de servicios como el correo electrónico, mensajería instantánea o redes sociales, así como la propia red que sustenta estas comunicaciones. Se trata de la llamada "ciberintervención", entendida como la captación en tiempo real del contenido de dichas comunicaciones sin interrupción de las mismas, así como de los datos de tráfico anejos.
A las medidas señaladas se tendrá que añadir la vigilancia policial de la propia red pública que sustenta esas comunicaciones, conocida como "ciberpatrullaje".

La intervención puede estar dirigida al contenido de la comunicación, a los datos de tráfico o a la información personal del usuario/abonado. Parte de la doctrina[11] distingue entre la "intercepción", dirigida a captar el contenido de la comunicación intervenida junto con los datos de tráfico y la "observación", destinada solamente a determinar la procedencia e identidad de los interlocutores o algunos de los datos de tráfico anexos al proceso comunicativo.

b) La segunda fuente de prueba corresponde a los dispositivos y sistemas informáticos de almacenamiento de datos, el acceso y registro para aprehender los datos relevantes

[8] Teresa ARMENTA DEU, *Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, whatsapp, redes sociales): entre la insuficiencia y la incertidumbre*; Isabel GONZALEZ CANO, *Derecho y Proceso*, Liber Amicorum Vol.II, edit. Atelier, Libros jurídicos, Barcelona 2018, p. 1084. Joaquín DELGADO MARTÍN (2016). *Investigación tecnológica y prueba digital en todas las jurisdicciones*, *La Ley*, ed. Digital, capítulo I y nota 5.

[9] Vicente GIMENO SENDRA , *La prueba preconstituida de la policía judicia*l, en VVAA., Problemas actuales de la Justicia Penal (Dir: Nicolás González-Cuellar Serrano), Colex, Madrid, 2013, p. 203.

[10] Teresa ARMENTA DEU, *Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, whatsapp, redes sociales): entre la insuficiencia y la incertidumbre*, Ob.Cit. p. 4.

[11] Nicolás CABEZUDO RODRIGUEZ (2015)*, Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal*, BMJ núm. 2186., p. 29.

contenidos en los mismos, calificado como "ciberregistro", y la orden de entrega a los depositarios de esos datos, si se trata de información retenida en poder de terceros[12].

La cesión de datos y archivos informáticos es una diligencia de investigación que consiste en la transferencia de informaciones y documentos en formato electrónico que obren en poder de particulares, entidades públicas o privadas.[13]

La medida analizada resulta controvertida en tanto en cuanto puede afectar a derechos fundamentales establecidos en la Carta, particularmente en los artículos 7 y 8 relativos a la intimidad personal y familia, entre otros[14]. Por este motivo será necesario realizar un análisis pormenorizado del tipo de datos que en cada caso pueden ser extraídos de los dispositivos electrónicos intervenidos. En orden a facilitar la labor indicada, tanto la Fiscalía[15] como el propio legislador europeo[16] han ofrecido definiciones técnicas de los elementos tecnológicos que contienen nuestros dispositivos.

---

[12] Corresponden a las medidas de investigación tecnológica previstas en el Convenio sobre Cibercrimen, ratificado por España el 20 de mayo de 2010 (arts. 16-21 y 29).

[13] Nicolás CABEZUDO RODRIGUEZ, *Ciberdelincuencia* ...Ob. Cit, p. 47. En este sentido es necesario distinguir la cesión de datos con la recogida de datos. Esta última medida se refiere a la labor de investigación realizada por la policía cuando sea absolutamente necesario para los fines de una investigación concreta (art. 22.3 LOPD) o que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

[14] Derecho al secreto de las comunicaciones, a la libertad de expresión, a la protección frente al uso de la informática, a la protección de datos, a la buena administración, a circular y residir libremente en el territorios de los estados miembros, a la libertad ideológica, libertad sindical, secreto profesional

[15] Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal, 2/2019, sobre interceptación de comunicaciones telefónicas o telemáticas, 3/2019, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, 4/2019, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización y 5/2019, sobre registro de dispositivos y equipos informáticos, además del Dictamen 1/19 Unidad de Criminalidad Informática de la Fiscalía General del estado acerca del alcance de la reclamación de datos de titulares, terminales y/o dispositivos de conectividad prevista en el nuevo art. 588 ter m de la Ley de Enjuiciamiento Criminal.

[16] De conformidad con el art. 2 de la Directiva 2002/58 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 telecomunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) se aplicarán las definiciones de la Directiva 95/46/CE, de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002 que se exponen a continuación:

Datos: los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario.

Datos de tráfico: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma.

Datos de localización: cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.

Comunicación: cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público.

En ese sentido, mientras que hay datos que permiten identificar la titularidad y geolocalización del dispositivo, otros van asociados al proceso comunicativo, a la identificación de los interlocutores, la duración, contenido y tiempo de producción de la comunicación estricta, distinguiendo a su vez la comunicación que tiene carácter dinámico con la que tiene carácter estático. Así, podemos afirmar que el primer grupo de datos-identificación de la titularidad y geolocalización- no suponen a priori una intromisión excesiva a la esfera personal del investigado ya que no permiten deducir conclusiones sobre la vida privada de las personas sujetas a las medidas. Por el contrario, el resto de datos permiten obtener además de la información necesaria para la investigación del delito, otros datos que en modo alguno resultan relevantes en la fase instrucción y lesionan gravemente el derecho a la intimidad, entre otros.

3. Derechos afectados

A través de esta diligencia, se obtiene una información que, considerada en su conjunto, puede permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan[17]. A continuación, exponemos los principales derechos[18] que pueden verse comprometidos de adoptarse la medida analizada:

Usuario: toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público, con fines privados o comerciales, sin haberse necesariamente abonado a dicho servicio.

Servicio telefónico: las llamadas (incluida la transmisión de voz, buzones vocales, conferencias y datos), los servicios suplementarios (incluido el reenvío o transferencia de llamadas) y los servicios de mensajería y servicios multimedia (incluidos los servicios de mensajería cortos, servicios multimedia avanzados y servicios multimedia).

Identificador de usuario: un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a Internet o a un servicio de comunicaciones por Internet, o de su registro en uno de dichos servicios.

Identificador de celda: la identidad de la celda desde la que se origina o termina una llamada de teléfono móvil.

Llamada telefónica infructuosa: una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación o en la que ha habido una intervención por parte del gestor de la red.

[17] STJUE, de 8 de abril de 2014, apartado 27.

[18] Existen otros derechos eventualmente vulnerados como el derecho a la libertad ideológica (STC 22 de mayo de 2019), libertad sindical (SSTC 11/1998, de 13 de enero y 60/1998, de 16 de marzo, 124/1998, de 15 de junio, libertad de información o secreto profesional (STEDH Sommer c. Alemania, de 27 de abril de 2017) e incluso el derecho a la tutela judicial efectiva (STC 96/2012, de 7 de mayo).

a) Derechos de la esfera personal: derecho a la vida privada y familiar, derecho al secreto de las comunicaciones y libertad de expresión, derecho a la protección frente al uso de la informática

La incidencia en la vida privada y familiar resulta indiscutible[19] al colisionar con los derechos propios de la esfera personal tales como el derecho al honor, a la intimidad personal y familiar y a la propia imagen, recogidos en los arts. 18 CE[20] y 6 y 7 de la CEDF[21]. El TEDH ha declarado reiteradamente que no le resultaba ni posible ni necesario tratar de definir de manera exhaustiva el concepto de "vida privada[22]". No obstante, se trata en cualquier caso, de un concepto amplio[23].

Por otro lado, la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ese extremo puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante,[24] hecho que repercutirá de forma indirecta en su libertad de expresión[25]. Por lo tanto, sino se garantiza el secreto de las comunicaciones para proteger el derecho a la vida privada, en el sentido de preservar al individuo un ámbito de actuación libre de injerencias de terceros, se puede producir una vulneración del derecho a la libertad de expresión.

Se configura así como una garantía formal, esto es, que protege la reserva o privacidad afecta a cualquier procedimiento de intercomunicación privada practicable con medios técnicos en uso, sea cual sea el contenido de la misma.

Cabe realizar la precisión efectuada por el TC[26] al declarar que el secreto de las comunicaciones no afecta a los partícipes en la comunicación, sino sólo a los terceros ajenos a ella. Los partícipes podrían quedar afectados directamente, en su caso, por el respeto a la vida privada e intimidad de su interlocutor.

Habida cuenta el peligro real y efectivo que la acumulación de datos sobre las personas puede representar sobre la libertad y derechos de los ciudadanos y, en especial, sobre su vida privada, el legislador estableció límites al uso de la informática, garantizando en cualquier caso el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (art. 18.4 CE).

---

[19] STEDH de 4 de diciembre de 2008, asunto S. y Marper c. Reino Unido.

[20] SSTC 254/1993, de 20 de julio, y 292/2000, de 30 de noviembre.

[21] Es conveniente aclarar que no toda intromisión en los derechos a la propia imagen o a la intimidad personal o familiar suponen a su vez una injerencia en el derecho al honor pero se expone a fin de justificar la máxima amplitud de los efectos que puede conllevar la medida.

[22] STEDH Niemietz c. Alemania de 16 de diciembre de 1992.

[23] STEDH Il Pretty c. Reino Unido de 19 de abril de 2002.

[24] Conclusiones del abogado general puntos 52 y 72 STJUE 8 abril 2014.

[25] El carácter negativo de este derecho, determina un ámbito de libertad frente al Estado en el seno del cual el individuo no puede ser importunado (SSTC 6/1981 y 86/1982).

[26] STC 114/84, de 29 de noviembre.

Paralelamente, el tratamiento informático de esos datos debe realizarse a través de ficheros o bien de forma automatizada, cumpliendo en todo caso los requisitos y garantías de veracidad, exactitud, actualización y rectificación. La Agencia de Protección de Datos será la autoridad responsable de su control.

b) El nuevo derecho a la protección de datos y al entorno virtual

A pesar de estar incluido en la esfera personal merece mención a parte el derecho a la protección de datos personal por su especial relevancia en la presente investigación. La jurisprudencia[27] ha reconocido su carácter autónomo e independiente pero resulta imprescindible su consolidación como derecho fundamental para garantizar el pleno respeto a la dignidad humana y el libre desarrollo de la personalidad[28]. No se trata de un derecho absoluto sino que al ser considerado en relación con su función en la sociedad[29] puede limitarse, respetando en todo caso el principio de proporcionalidad.

Íntimamente relacionado con el anterior, la jurisprudencia ha desarrollado el "derecho al entorno virtual"[30], entendido como toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Ese espacio de exclusión es, además, susceptible de ampliación o reducción por el propio titular.[31]

En cuanto al ámbito normativo con carácter general está el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a las personas físicas en lo que respecta al tratamiento de datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (RGPD), siendo su reflejo nacional la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Con carácter específico se tramitó la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa ala protección de las personas físicas en los 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 Marco2008/977 JAI del Consejo. Al estar en la actualidad en vías de trasposición, es la LO 15/1999, de 13 de diciembre que en sus

[27] SSTC de 22 de mayo de 2019 y 292/2000, de 30 de noviembre.

[28] Julio PEREZ GIL (2019), "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal" en "Justicia: ¿Garantías versus Eficiencia?" (Dir. Jiménez Conde y Bellido Penadés), edit. Tirant lo Blanch, Valencia, pp. 400 y 401.

[29] Casos C-92 and C-93/09, Volker und Markus Schecke GbR y Harmut Eifert c. Land Hessen (Gran Sala), 9 de noviembre 2010.

[30] STEDH de 30 de mayo de 2017 (Recurso nº 32600/12), entre otras.

[31] STS 287/2017, de 19 de abril.

artículos 22 y 23 regula las especialidades que tiene el tratamiento de datos personales en el ámbito judicial penal y policial.[32]

No obstante, hay que atender a los efectos que despliega la Directiva indicada en nuestro ordenamiento jurídico sea mediante el principio de interpretación conforme a la directiva, sea mediante el posible efecto directo de la misma.[33] De un lado, por el principio de interpretación conforme a la Directiva, los jueces tienen la obligación de interpretar el Derecho interno a la luz y finalidad de dicha norma, para alcanzar el resultado del art. 189 TUE. De otro, el posible efecto directo tiene lugar cuando no se haya traspuesto la Directiva antes del plazo correspondiente o bien cuando la aplicación se refiera a disposiciones sean incondicionales y suficientemente claras y precisas, que contemplen derechos a los ciudadanos.[34]

Como derecho reconocido en el art. 8 CEDF dispone de una doble vía de protección[35]. De un lado, la de carácter personal, la vía garantista general, en orden a preservar antes la libre circulación de datos personales, los derechos de información, acceso, rectificación, cancelación y oposición que requerirá en todo caso, del consentimiento expreso para su tratamiento, la satisfacción de intereses legítimos del responsable del tratamiento, entre otros condicionantes previstos en el art. 6 RGPD; y la vía excepcional o especial, relacionada con la represión, la investigación y enjuiciamiento del delito, que requiere un tratamiento especial en cuanto se trata de medios de investigación y obtención de fuentes probatorias preconstituidas y, en definitiva, de prueba de cargo para la imposición de consecuencias jurídicas sancionadoras de naturaleza penal, que no necesitará del consentimiento expreso de sus titulares debido a su finalidad[36].

Conviene atender a la categorización de los datos en función de la legítima expectativa de la intimidad[37]. Así, encontramos datos relativos a la intimidad más cerrada, referido a informaciones que no deberían ser utilizadas como prueba; datos secretos, en los que hay una alta expectativa de confidencialidad; datos confidenciales compartidos con personas de confianza; datos con accesibilidad limitada, con la expectativa de confidencialidad atenuada y finalmente datos con accesibilidad ilimitada, sin expectativa de privacidad alguna. Esta clasificación permitiría verificar el test de proporcionalidad de cualquier medida de investigación o prueba que tenga como objeto la obtención de datos electrónicos[38].

---

[32] Compartimos con Julio PEREZ GIL la indeterminación excesivamente amplia de la norma no basada en criterios objetivos (*Exclusiones probatorias por…*", Ob. Cit., p. 410).

[33] Joaquín DELGADO MARTÍN (2019), *La protección de datos personales en el proceso penal: Directiva 2016/680*, https://elderecho.com/la-proteccion-datos-personales-proceso-penal-directiva-2016-680, Consulta de 27 de febrero de 2019.

[34] STC 292/2000, de 30 de enero de 2016.

[35] Pilar SOLAR CALVO (2012), *La doble vía europea en protección de datos*, en la Ley, nº2832.

[36] Isabel GÓNZALEZ CANO, *Derecho y Proceso*…Ob. Cit., pp. 1092 y 1903.

[37] Claudia WARKEN, *Classification of Electronic Data for Criminal Law Purposes*, Eu Crim 2018/4 (http://doi.org/10.30709/eucrim-2018-023/).

[38] Julio PÉREZ GIL, *Exclusiones probatorias por…*Ob. Cit., p. 425.

c) Otros derechos propios del ámbito comunitario: derecho a la buena administración y el derecho a circular y residir libremente en el territorio de los Estados miembros

En el marco del derecho a la buena administración, las autoridades públicas[39] realizan tratamientos de datos de carácter personal en muchas de sus actividades y, por ello, también actúan como responsables y encargados del tratamiento. Así pues, la normativa vigente en protección de datos también les es de aplicación en virtud del art. 41 de la CEDF. En cuestión de protección de datos serán las responsables de la calidad de los datos, de la aplicación de los principios de proporcionalidad a las solicitudes registradas, así como su limitación a los fines compatibles.

El derecho a circular y residir libremente en el territorio de los Estados miembros es una de las ventajas más evidentes y preciadas de la Unión Europea para sus ciudadanos. Unos 13 millones de ciudadanos de la Unión han hecho uso del mismo y viven actualmente en otro país de la Unión. Los ciudadanos de la Unión también realizan cada año más de 1 000 millones de desplazamientos a otros países de la Unión por negocios o placer sin someterse a controles en el espacio Schengen o beneficiándose de controles rápidos en las fronteras[40]. El artículo 21, apartado 1, del Tratado de Funcionamiento de la Unión Europea establece que todo ciudadano de la Unión tiene el derecho de circular y residir libremente en el territorio de los países de la Unión, con las limitaciones y condiciones dispuestas en los Tratados y según las medidas adoptadas al efecto. Sin embargo, no podemos olvidar que lleva aparejada la existencia de la delincuencia transfronteriza o trasnacional, que necesitará de una respuesta conjunta por parte de la Unión Europea.

4. Eficacia y garantías de la cesión de datos

La controversia que origina la adopción de la medida obliga a abordar los mandatos efectuados por el legislador destinados a asegurar la eficacia de la misma de un lado, así como a las garantías en su adopción, de otro. En definitiva, se pretende que la obtención de datos sea compatible con los derechos reconocidos en la Carta y constituya una herramienta idónea para la prevención y persecución de la delincuencia.

En cuanto a la eficacia, la normativa europea establece dos fases en la que se desarrolla la medida. La primera es la obligación por parte de los operadores de telecomunicaciones de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación. La segunda, completando a la anterior, es el deber de entrega o cesión de dichos datos a los agentes facultados siempre que les sean

[39] Descartamos en consecuencia que este tratamiento de datos lo puedan realizar empresas privadas cuyo interés no será defender el derecho a la protección de datos o a la intimidad, sino más bien de carácter comercial (ELS DEL BUSSER, *La creciente involucración de las empresas privadas en las investigaciones penales de la UE*, en Ignacio COLOMER HERNANDEZ I.(Dir.) y Sabela OUBIÑA BARBOLLA (Coord.), *La transmisión de datos*…Ob. Cit., p. 399.

[40] Libertad de circulación y residencia en Europa. Guía de tus derechos de ciudadano de la Unión, Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2013, p. 5.

requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

Por lo que se refiere a las garantías necesarias para impedir su manipulación, acceso indebido o destrucción, los Estados se obligan en arbitrar las pautas idóneas para el aseguramiento de los datos conservados de tal forma que aseguren la integridad y confidencialidad de los mismos[41]. La legalidad y licitud en el tratamiento de datos es fundamental para su uso adecuado y lícito en una causa penal.

En consecuencia, las autoridades pertinentes tendrán que adoptar las medidas técnicas y organizativas que permitan una protección real de los datos personales intervenidos, asegurando su exactitud y actualidad, así como eliminando los riesgos de su posible destrucción, pérdida o acceso no autorizado, alteración o divulgación.

En este sentido, los datos de carácter personal deberán eliminarse cuando ya no sean necesarios para el fin con que se transmitieron o cuando haya vencido su plazo de conservación según lo dispuesto en la legislación nacional. En consecuencia, nuestro legislador estableció en el art. 588 bis k LECrim las reglas sobre destrucción de los datos. Se establece que una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. No obstante, se conservará una copia bajo custodia del Letrado de la Administración de Justicia. *Asimismo, s*e acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal. La destrucción se autorizará judicialmente mediante las órdenes oportunas que dicte el Juez a la Policía Judicial.

5. Regulación

5.1. Aplicabilidad del derecho nacional - derecho europeo

El origen de la regulación de estas medidas establecidas actualmente en la LECrim se lleva a cabo por primera vez en la Directiva 2006/24/CE sobre conservación de datos relativos a las comunicaciones. En nuestro ordenamiento jurídico se incorporó mediante la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes de comunicación.

En la directiva europea se regulaba la obligación de conservación de datos relativos a las comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones de forma generalizada e indiferenciada, por lo que dio lugar a que fuera declarada ilegal por parte del TJUE[42]. La razón ofrecida por el tribunal respondía a que no garantizaba la protección del

[41] Este hecho implicará además, el compromiso de colaboración de las entidades públicas y privadas de carácter nacional e internacional como la Agencia de Protección de Datos, Comisión del Mercado de las Comunicaciones, operadores y proveedores de servicios de Internet, etc.

[42] Los motivos que llevaron a la declaración de ilegalidad fueron: inexistencia de limitaciones de cualquier índole la conservación de datos, indefinición del concepto delito grave, falta de reglas sobre las autoridades con facultades para acceder y utilizar tales datos conservados, ausencia de medidas de seguridad exigibles

ciudadano frente al abuso o acceso indebido o ilícito a los datos conservados, al resultar comprometidos los ya citados arts. 7 y 8 de la CDFUE[43].

Siendo una norma proclamada ilegal por el TJUE, se abre el debate en torno a la validez de las normas internas de trasposición de la misma que hicieron posible su integración en el ordenamiento jurídico nacional. A pesar de que la relación entre las normas comunitarias y las normas internas no será objeto de estudio en este trabajo, resulta conveniente justificar las razones por las que declaración de ilegalidad de la mencionada directiva no condicionó la vigencia de las normas internas que la traspusieron. En síntesis, podríamos sostener que mientras que la Directiva, hacía un tratamiento excesivamente amplio y general en materia de conservación de datos de comunicaciones, las normas internas que la desarrollaban regulaban de una forma exhaustiva y detallada ese mismo extremo. En consecuencia, las causas que justifican la anulación del texto comunitario por parte del Tribunal[44] -basadas principalmente en la amplia laxitud- no son extrapolables a la Ley 25/20017, que minuciosa y pormenorizadamente en su contenido, regula tanto el deber de conservación de los datos como la obligación de entrega de los mismos, garantizando de forma efectiva los derechos de los particulares.

Como resultado de la declaración de ilegalidad indicada, cobró vigencia a los efectos de aplicabilidad, la regulación anterior a la misma, es decir, 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), en su versión modificada por la Directiva 2009/136/CE Parlamento Europeo y del Consejo, de 25 de noviembre de 2009[45].

---

para acreditar la integridad y confidencialidad de los datos (STJUE, Gran Sala, de 8 de abril de 2014, casos C-293/2012 y C-594/2012)

[43] José Luis RODRIGUEZ LAINZ., *Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la Ley española sobre la conservación de datos relativos a las comunicaciones,* Diario La Ley, nº8308, Sección doctrina, 12 de mayo 2014, Ref. D-148, Editorial LA LEY, p. 1/13.

[44] Los motivos expuestos por el alto tribunal son los siguientes:

- Universalización de la recogida de datos: se refiere a la conservación de todos los datos de tráfico relativos a la telefonía fija, la telefonía móvil, el acceso a internet, el correo electrónico por Internet y la telefonía por Internet.
- Afectación a usuarios no sospechosos pues se permite que se almacene una masa de tipo de datos con respecto a un número ilimitado de personas que comprende a todos los abonados y usuarios registrados.
- No garantía del cumplimiento de la finalidad de las medidas: al abarcar de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico, no se establece ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves.
- Los plazos de conservación en la directiva son extremadamente imprecisos, dejando al arbitrio de cada estado su determinación de entre 6 meses y 2 años.
- Tampoco se establece los niveles de protección que aseguren los datos conservados frente a riesgos de abuso o uso o acceso ilegal a los mismos. Sería conveniente que se arbitraran mecanismos que garanticen la integridad y la confidencialidad de los datos.

[45] José Luis RODRIGUEZ LAINZ niega la relación de sucesividad mediante la cual la norma posterior invalidada sustituía a una anterior, derogándola. En el caso concreto, la Directiva 2006/24/CE introducía una norma de remisión (ap. 1 bis) respecto del art. 15.1 Directiva 2002/58/CE. ("Sobre la incidencia…", Ob. Cit. p.3/13)

En el curso de la tramitación de la cuestión prejudicial-que abordaremos en los próximos epígrafes- se promulgó la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, incorporando la normativa recientemente analizada. Particularmente, el TJUE en su resolución a la cuestión planteada, interpretó el alcance de los arts. 579 y 588 ter j.

5.2. Competencia del TJUE y protección de los derechos fundamentales

a. Consideraciones generales

Resulta imprescindible tratar la adecuación de competencia del TJUE ya que los parámetros que integran estándar de protección de los derechos fundamentales a los que afecta la medida de investigación son de distinta intensidad en función de si se está aplicando el derecho comunitario o el derecho interno.

Existe por lo tanto, una divergencia entre los estándares de garantías establecidos respecto a la transferencia transfronteriza de datos personales y el nivel garantista del derecho interno para su tratamiento dentro de su propio estado[46] .

Ante una cuestión propia del derecho interno, corresponde atenerse a lo establecido en nuestra LECrim y la CE, siendo el Tribunal Constitucional el órgano competente para elaborar los criterios interpretativos de las normas aplicables en lo relativo a derechos fundamentales; mientras que ante una cuestión de derecho comunitario, habrá que estar a lo establecido en la Carta y podremos afirmar la competencia del TJUE para la resolución de las cuestiones interpretativas que se puedan plantear en materia de derechos fundamentales.

De conformidad con el art. 51 de la Carta, los derechos fundamentales garantizados en el ordenamiento comunitario deben ser aplicados en todas las situaciones reguladas por el Derecho de la Unión, pero no fuera de ellas. El desarrollo jurisprudencial[47] permite afirmar que estamos ante supuestos de derecho comunitario si un Estado aplica una norma cuya naturaleza es de aplicabilidad directa, así como cuando traspone cuando traspone una directiva comunitaria a su ordenamiento interno e incluso cuando quiere excepcionar en algún ámbito la aplicación de la norma comunitaria[48].

Igualmente, el TJUE ha realizado una interpretación extensiva en la aplicación del derecho comunitario entendiendo integrados incluso aquellos supuestos en los que aún no trasponiéndose una directiva, una norma nacional esté dirigida a dar cumplimiento a obligaciones impuestas en los Tratados a los Estados miembros[49].

[46] Isabel GONZALEZ CANO, *Derecho y Proceso*..., Ob. Cit., p. 1082.

[47] SSTJUE de 15 de noviembre de 2011, caso Dereci y otros, asunto C-256/11, apartado 72, y de 7 de junio de 2012, caso Vinkov, asunto C-27/11, apartado 58.

[48] Art. 288 Tratado de Funcionamiento de la Unión Europea en el que se establece que La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y los medios.

[49] STJUE 26 de febrero de 2013, caso Aklagaren contra Hans Akerberg Fransson, asunto C-617/10, apartado 28.

En la práctica forense en cuanto al control de convencionalidad[50] llevado a cabo por la jurisdicción ordinaria, cuando un juez nacional, en el marco de un proceso, debe ceñirse al derecho de la unión, atenderá a los derechos contemplados en la Carta, comportando esta forma, la inaplicación de la norma nacional si ésta contradice los derechos fundamentales. Podrá en su caso, plantear una cuestión prejudicial al TJUE para solicitar una interpretación autorizada de los derechos a efectos de controlar la norma nacional[51].

Eventualmente, en el desarrollo de ese control de convencionalidad, el juez nacional puede entender que la norma aplicable vulnera derechos reconocidos en la Carta e igualmente presente vicios de inconstitucionalidad, al ser contraria a la CE. En esa circunstancia, al amparo de lo dispuesto en el art. 267 TFUE, se podrá también acudir al TJUE sin la previa resolución del TC[52].

La multitud de normas reguladoras de los diferentes sistemas de intercambio y facilitación de datos de carácter personal con fines penales ha devenido un verdadero *patchwork* normativo[53], cuya complejidad requiere de una labor unificadora por parte del legislador. Ante el panorama descrito se evidencia la necesidad de armonización de las disposiciones nacionales y comunitarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales, en particular del derecho a la intimidad y a la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas[54].

b. Consideraciones particulares en la diligencia de cesión de datos

La última cuestión[55] suscitada en torno al criterio de la proporcionalidad se origina a causa de una investigación llevada a cabo por parte de un Juzgado de Instrucción para el esclarecimiento del robo violento de un teléfono móvil[56]. Los hechos descritos justificaron que la policía judicial solicitara la práctica de la diligencia consistente en recabar de las diversas operadoras telefónicas datos relacionados con el número del móvil sustraído. El Juez denegó dicha diligencia por dos motivos: la escasa idoneidad de la diligencia para averiguar e identificar a los responsables del robo y el hecho de que la previsión normativa establece que la práctica de la medida sólo es oportuna en caso de delitos graves. Notificada la resolución judicial denegatoria, el Ministerio Fiscal interpuso un recurso de apelación amparándose en que la diligencia instada ya se había llevado a cabo en supuestos anteriores de características similares[57]. En este contexto podríamos

[50] Pablo NUEVO LÓPEZ (2015), *Control de convencionalidad y aplicación judicial de los derechos fundamentales de la Unión Europea*, Revista de Dret Públic, nº 50.

[51] Araceli MANGAS MARTÍN (2008), *Artículo 51. Ámbito de aplicación*, en *Carta de los derechos fundamentales de la Unión Europea. Comentario artículo por artículo*, edit. Fundación BBVA, p. 818.

[52] STJUE de 22 de junio del 2010, asuntos acumulados C-188/10 y C-189/10, apartados 44 al 55.

[53] Alfonso GALÁN MUÑOZ., "La protección de los datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea" en Ignacio COLOMER HERNÄNDEZ y Sabela OUBIÑA BARBOLLA (2015), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Edit. Aranzadi, Navarra, p.51.

[54] STJUE de 21 de diciembre 2016, apartado 68.

[55] Cuestión prejudicial C-207/16.

[56] Utilizamos a modo de ejemplo el supuesto concreto por la actualidad del mismo, así como por ser altamente frecuente en los órganos judiciales la cuestión suscitada.

[57] STS 745/2010, de 26 de julio.

entender que la cuestión planteada no se refiere a la aplicación del derecho comunitario por considerar que queda excluido de forma expresa de la Directiva 1995/46 (art. 3, apdo. 2)[58] y de la Directiva 2002/46 (art. 1, apdo. 3)[59].

Ciertamente el TJUE[60] ha declarado que una medida que regula el acceso de las autoridades nacionales a los datos conservados por los proveedores de servicios de comunicaciones electrónicas está incluida en el ámbito de aplicación de la Directiva 2002/58. Sin embargo, el acceso por parte de la policía judicial a esos datos, en el marco de la investigación de un delito, requiere de una previa autorización judicial, de manera que constituye una actividad del Estado en materia penal. Por lo tanto, estaría incluido en las excepciones previstas en el art. 1, apdo. 3 de la Directiva 95/46[61].

En apoyo a este argumento, cabría añadir que si partimos de la negación de la relación de interdependencia entre las normas comunitarias de las que las trasponen a los ordenamientos internos, porque-como hemos visto anteriormente- estas han adquirido una vigencia propia que no se ve afectada por una declaración de ilegalidad de la norma comunitaria, entonces también podemos afirmar que no se está aplicando el derecho de la Unión sino que estamos ante un supuesto de derecho interno que debemos resolver de acuerdo con nuestras normas nacionales. Así las cosas, el parámetro para determinar si los derechos fundamentales resultan salvaguardados serían el art. 18 de la CE y la LECrim en lugar de los arts. 7 y 8 de la Carta.

En sentido contrario, se pronunció el abogado general en sus conclusiones[62] defendiendo la competencia del TJUE al entender que es un asunto cuya aplicación del Derecho de la Unión es preceptiva. La razón alegada fue que las legislaciones nacionales sobre conservación de datos, a efectos de la lucha contra la delincuencia, están incluidas en el ámbito de aplicación de la Directiva 2002/58 no sólo en la medida en que definen las obligaciones de las autoridades nacionales en ese ámbito, sino también en la medida en que regulan el acceso de las autoridades nacionales a los datos conservados en este marco[63]. Asimismo, en base a esta tesis es importante no confundir entre los datos personales tratados directamente en el marco de las actividades del Estado de carácter reservado en un ámbito incluido en el Derecho penal y por otro, las tratadas en el marco de las actividades de naturaleza mercantil de un prestador de servicios de comunicaciones electrónicas que después emplean las autoridades estatales competentes.

Finalmente, el TJUE corroboró su competencia basando la misma en las resoluciones anteriores[64] que incluían dentro del ámbito del derecho de la Unión, la conservación de los datos por parte de

[58] Se establece en el precepto señalado que las disposiciones de dicha norma no se aplicarán al tratamiento de datos personales que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal.

[59] En el mismo sentido que la Directiva mencionada supra.

[60] STJUE de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15.

[61] STJUE de 2 de octubre, asunto 207/16, apartado 45.

[62] Conclusiones del Abogado General Sr. Henrik Saugmandsgaard presentadas el 3 de mayo, asunto C. 207/16, apartado 46.

[63] STJUE de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15.

[64] STJUE de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, apartados 75 y 76.

los proveedores de servicios de comunicaciones electrónicas y el acceso de las autoridades nacionales a esos datos, por lo tanto, será el criterio a seguir en situaciones futuras.

6. Fundamento jurídico de la medida en el ordenamiento de la UE

6.1. Construcción de una Europa de Libertad, Seguridad y Justicia

Para justificar la adopción de la injerencia es imprescindible aludir a la necesidad de consolidación de la Unión Europea no solo como Unión en materia económica, sino como una verdadera Europa de Libertad, Seguridad y Justicia. La construcción de esa Europa implica combatir la delincuencia transfronteriza, cuyas formas de perpetración son cada vez más sofisticadas en atención a la evolución tecnológica que hemos apuntado al principio de este estudio.

También la jurisprudencia del Tribunal de Justicia establece que la lucha contra el terrorismo internacional es fundamental para el mantenimiento de la paz y seguridad internacional, a la vez que es un objetivo de interés general de la Unión[65]; y lo mismo ocurre en lo que respecta a la lucha contra la delincuencia grave para garantizar la seguridad pública[66]. Por su parte, el art.6 de la Carta reconoce el derecho de toda persona no sólo a la libertad, sino también a la seguridad.

A causa del crecimiento significativo de las posibilidades de comunicaciones electrónicas, el Consejo de Justicia e Interior de 19 de diciembre de 2002 consideró que los datos relativos al uso de las comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en prevención de delitos y la lucha contra la delincuencia, en especial delincuencia organizada[67].

6.2. Principios de cooperación en materia penal, reconocimiento mutuo y confianza entre los Estados

Conforme al principio de cooperación leal, la Unión y los Estados miembros se respetarán y asistirán mutuamente en el cumplimiento de las misiones derivadas de los Tratados. A tal fin, los Estados miembros adoptarán todas las medidas generales o particulares apropiadas para asegurar el cumplimiento de las obligaciones derivadas de los Tratados o resultantes de los actos de las instituciones de la Unión (arts. 3 y 4 TUE) y se abstendrán de toda medida que pueda poner en peligro la consecución de los objetivos de la Unión.

La cooperación judicial en materia penal se basa en el principio de reconocimiento mutuo de las sentencias y resoluciones judiciales e incluye medidas para armonizar las leyes de los Estados miembros en diversos ámbitos. (Arts. 82 a 86 TFUE)[68].

---

[65] STJUE de 3 de septiembre de 2008, asuntos acumulados C-402/05 P y C-415/05 P, EU:C:2008:461, apartado 363, y Al-Aqsa/Consejo, C-539/10 P y C550/10 P, EU:C:2012:711, apartado 130).

[66] STJUE de 23 de noviembre de 2010, asunto C-145/09.

[67] STJUE de 8 de abril, asuntos acumulados C-293/12 y C-594/12, apartado 43.

[68] El principio de reconocimiento mutuo, basado en la confianza mutua entre los Estados miembros y consagrado en el Consejo Europeo de Tampere como la «piedra angular» de la cooperación judicial civil y penal en la Unión Europea, ha supuesto una auténtica revolución en las relaciones de cooperación entre los Estados miembros, al permitir que aquella resolución emitida por una autoridad judicial de un Estado

Entendemos el reconocimiento mutuo como aquél que permite a las autoridades judiciales españolas que dicten una orden o resolución comprendida en el ámbito objetivo de la LRM 23/2014 transmitir dicha orden o resolución "a otro Estado miembro para su reconocimiento y ejecución" (aspecto activo del principio); o que impone a las autoridades judiciales españolas competentes el reconocimiento y ejecución en España, dentro del plazo previsto, de «las órdenes europeas y resoluciones penales previstas en esta Ley cuando hayan sido transmitidas correctamente por la autoridad competente de otro Estado miembro y no concurra ningún motivo tasado de denegación del reconocimiento o ejecución» (aspecto pasivo del principio)[69].

La promoción del reconocimiento mutuo pasa por la confianza jurídica entre los estados[70]. Así, a pesar de que los conceptos de armonización y reconocimiento mutuo pueden resultar contradictorios, la existencia de unos mínimos comunes facilita el reconocimiento mutuo[71].

La homogeneización de las garantías de las personas afectadas por estos procedimientos favorecerá la construcción de una base sólida y eficaz para la cooperación transfronteriza.

6.3. Principio de disponibilidad de datos

En este contexto nace el principio de disponibilidad de datos por el que las autoridades competentes de los Estados de la UE tendrían acceso y podrían disponer de las informaciones en materia de investigación y enjuiciamiento penal, en las mismas condiciones con las que cuenta el estado en el que la información se obtiene o está registrada[72].

El principio de disponibilidad supone, por una parte, la obligación de tener los datos disponibles y cederlos a estos fines, de acuerdo con el principio de especialidad; y por otra, la posibilidad de que esta cesión de datos no venga regida con carácter general por el principio de especialidad, es decir, la posibilidad de que la autoridad del Estado cesionario los utilice para investigar o enjuiciar un delito diferente de los alegados para solicitar y justificar la cesión[73].

Son varias las normas comunitarias[74] que recogen la importancia de este principio, siendo la Decisión 2008/615/JAI, del Consejo, de 23 de junio, sobre la profundización de la cooperación

---

miembro sea reconocida y ejecutada en otro Estado miembro, salvo cuando concurra alguno de los motivos que permita denegar su reconocimiento. Finalmente, el Tratado de Funcionamiento de la Unión Europea ha supuesto la consagración como principio jurídico del reconocimiento mutuo, en el que, según su artículo 82, se basa la cooperación judicial en materia penal (Preámbulo I, LRM, 23/2014, de 20 de noviembre).

[69] De conformidad con el art.1 de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.

[70] Conclusiones del Consejo sobre reconocimiento mutuo en materia penal (2018/C 449/02)

[71] Francisco SOTO NIETO (2005), *Fundamentos constitucionales del derecho penal europeo", Revista General del Derecho Penal*, núm. 3.

[72] Alfonso GALÁN MUÑOZ, *La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea*, en VVAA (Dir. Ignacio COLOMER HERNÁNDEZ), *La transmisión de datos personales*..., Ob. Cit, pp.42 y ss.

[73] Isabel GONZÁLEZ CANO, *Derecho y Proceso*... Ob. Cit., p. 1076.

[74] Decisión del Consejo 2008/633/JAI, de 23 de junio de 2008, Decisión Marco 2008/315/JAI de 26 de febrero o Decisión del Consejo 2009/616/JAI, de 6 de abril.

transfronteriza[75], en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza y la Decisión Marco 2006/960/JAI, del Consejo, de 18 de diciembre, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, las que favorecen su integración al garantizar la disponibilidad de un amplio y variado número de informaciones a todos los organismos nacionales y europeos dedicados a la investigación y prevención de delitos[76].

Por último, en relación a la obtención transfronteriza de datos, cobra especial relevancia la Orden Europea de Investigación[77] entendida como instrumento jurídico básico para la obtención de prueba penal entre Estados miembros de la Unión Europea, con fundamento en el principio de reconocimiento mutuo. Supone un avance respecto al Exhorto de obtención de pruebas ya que no se limita a la solicitud de pruebas a otro estado, sino que además se interesa que se realice de conformidad con las exigencias particulares de protección de derechos fundamentales de cada uno de los estados miembros.

7. La evolución del principio de proporcionalidad en torno a la cesión de datos a la luz de la jurisprudencia del TJUE

Hemos observado que la conservación de los datos y su posterior orden de entrega ha ido evolucionando a lo largo de los años. El TJUE- mediante tres resoluciones esenciales- ha ido elaborando una interpretación precisa sobre el tratamiento de los datos almacenados por los servicios y operadores de telecomunicaciones y el principio de proporcionalidad, interpretación que debe ser tenida en cuenta en la adopción de la medida por parte de los órganos investigadores.

7.1. Principio de proporcionalidad en relación al principio de disponibilidad de datos

La primera de las resoluciones que conforman este compendio interpretativo respecto de la medida en cuestión es la STJUE de 8 de abril de 2014, cuya finalidad es valorar la compatibilidad entre 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 comunicaciones y la Carta.

La norma objeto de enjuiciamiento por el tribunal, en su contenido permite el almacenamiento de gran cantidad de tipos de datos respecto a un número ilimitado de personas, en un periodo temporal indefinido. La conservación de los datos afecta casi exclusivamente a personas cuyo comportamiento no justifica en modo alguno la conservación de datos referentes a ellas. Estas personas están expuestas al riesgo añadido de que las autoridades investiguen sus datos, conozcan su contenido, se informe sobre su vida privada y utilicen esos datos para múltiples fines, teniendo en cuenta, en particular, el inconmensurable número de personas que tienen acceso a los datos durante un periodo mínimo de seis meses.

[75] Más conocida como la Decisión Prüm.

[76] Afonso GALÁN MUÑOZ, *La protección de…* Ob. Cit., p. 48.

[77] Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014-EDL 2014/60572, traspuesta a nuestro ordenamiento por la Ley 32018, de 11 de julio-EDL 2018/92374

El Tribunal en relación a la proporcionalidad de la injerencia constada en la Directiva establece las siguientes orientaciones a tener en cuenta:

1. En cuanto a la vulneración de derechos fundamentales relativos a la intimidad y protección de datos, la injerencia resulta apropiada y necesaria para el logro de los objetivos consistentes en la lucha contra la delincuencia grave, entendido como interés general de acuerdo con la Jurisprudencia del TJUE[78].

Se permite de esta manera que las autoridades nacionales competentes puedan disponer de más datos para el esclarecimiento de delitos atendiendo a la importancia creciente de los medios de comunicación electrónica.

Por lo que se refiere al carácter necesario, la lucha contra la delincuencia grave reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida, de las técnicas modernas de investigación. Sin embargo, en lo que respecta al derecho a la intimidad, la protección de este derecho fundamental exige en cualquier caso, conforme a la jurisprudencia reiterada del Tribunal de Justicia, que las excepciones a la protección de datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de lo estrictamente necesario[79].

2. Por lo que se refiere a los destinatarios de las medidas, el Tribunal advierte que no puede afectar con carácter global a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales. Menos aún cuando se aplica a personas cuyas comunicaciones están sujetas al secreto profesional.

Como condición previa es fundamental la existencia de indicios contra la persona sospechosa o investigada, la discriminación en función de la persona afectada, la localización geográfica que precise el uso de la medida, el tiempo necesario para conservar los datos, etc.

3. Debe establecerse una autoridad independiente para que controle el cumplimiento de los requisitos de protección y seguridad, a través de medidas técnicas y organizativas, teniendo en cuenta consideraciones técnicas y organizativas exigidas en el art. 8 apartado 3 de la Carta.

4. Se ha de asegurar protección eficaz de los datos conservados contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos respecto de tales datos. La implantación de estas medidas de seguridad no puede depender de consideraciones económicas. También se garantizará la destrucción definitiva de los datos al término de su periodo de conservación.

5. La disponibilidad se vincula al principio de especialidad, de manera que los datos recabados y cedidos lo sean en función una causa penal concreta.

7.2. Principio de proporcionalidad en relación al principio de especialidad en el tratamiento de datos personales

[78] Sentencias Afton Chemical, EU:C:2010:419, apartado 45; Volker und Markus Schecke y Eifert, EU:C2010:662, apartado 74; Nelson y otros, C-581/10 y C-629/10, EU:C:2012:657, apartado 71; Sky Österreich, C-283/11, EU:C:2013:28, apartado 50, y Schaible, C-101/12, EU:C:2013:661, apartado 29.

[79] Sentencia IPI, C-473/12, EU:C:2013:715, apartado 39.

Una vez declarada la ilegalidad de la Directiva, tienen lugar los asuntos acumulados C-203/15 y C-698/15, dictándose al respecto la STJUE de 21 de diciembre de 2016, que valoró la falta de idoneidad de las normativas nacionales que imponían a los proveedores una obligación general de conservación de datos y que prevén el acceso a 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.

Cobra importancia el principio de especialidad, que exige que una medida esté relacionada con la investigación de un delito concreto. Por lo tanto, no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva (art. 588 bis a) LECrim.

El TJUE precisa en este caso la delimitación del principio de especialidad en relación en base a dos elementos esenciales:

1. Prohibición de conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica. Es decir, se establece una previa clasificación de los datos a partir de la que se deberán tomar en cuenta con la única finalidad de luchar contra la delincuencia grave para determinadas personas afectas y por un plazo de tiempo limitado.

En consecuencia, con carácter previo, la conservación selectiva de datos y de localización a efectos de la lucha contra la delincuencia grave exigirá, según la doctrina del tribunal, de un lado, que el ordenamiento nacional disponga de normas claras y precisas en relación al alcance y aplicación de la medida concreta, así como el establecimiento de garantías suficientes frente al riesgo de abusos de datos personales. De otro lado, la adopción de la medida siempre debe tener carácter excepcional para casos estrictamente necesarios y obedecer a criterios objetivos, en los que se evidencie la relación entre los datos conservados y el fin perseguido.

2. Control previo por un órgano jurisdiccional o una autoridad administrativa independiente (art. 8 apartado 3 CDFUE), que corrobore el cumplimiento de los requisitos expuestos en el punto anterior y así como establezca las condiciones y procedimientos correspondientes, basados en criterios objetivos.

Así, se apremiará para que "los proveedores adopten medidas técnicas y de gestión adecuadas que permitan garantizar una protección eficaz de los datos conservados contra los riesgos de abuso y contra todo acceso ilícito a esos datos. Habida cuenta de la cantidad de datos conservados, del carácter sensible de esos datos y del riesgo de acceso ilícito a éstos, los proveedores de servicios de comunicaciones electrónicas deben garantizar, para asegurar la plena integridad y confidencialidad de esos datos, un nivel particularmente elevado de protección y de seguridad mediante medidas técnicas y de gestión adecuadas"[80].

7.3. Última vuelta de tuerca del principio de proporcionalidad respecto al tratamiento de datos personales en cuanto al alcance del delito grave

A pesar de las delimitaciones anteriores realizadas por la jurisprudencia europea, nos encontramos que en la actualidad el sistema de captación, recopilación y almacenamiento de

[80] STJUE de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15.

datos se lleva a cabo aún sin indicio penal alguno de comisión de un delito, y sin un catálogo preestablecido de delitos para los que podría acudirse a estas medidas, resultando por lo tanto insuficiente la referencia de la Directiva de delitos graves, sin ninguna otra precisión, catálogo o criterio al respecto.

En este panorama surge la cuestión C-207/16 mediante la que se acuerda elevar las siguientes cuestiones al TJUE:

Primera.- ¿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?

Segunda.- ¿En su caso, si se ajustara a los principios constitucionales de la Unión, utilizados por el TJUE en su sentencia de 8 de abril de 2014[81] 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?

Es decir, debemos conocer qué elementos hay que tener en cuenta para apreciar si los delitos respecto de los cuales puede autorizarse a las autoridades policiales, a efectos de investigación de un delito, a acceder a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, son de una gravedad suficiente para justificar la injerencia que supone tal acceso en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta[82], tal y como ha interpretado el TJUE en supuestos anteriores[83].

Cumplido lo anterior, en cuanto a su compatibilidad con los principios constitucionales de la Unión y que la determinación de la gravedad del delito atiende sólo a la pena imponible, habrá que averiguar si la previsión general de límite en tres años de prisión es compatible con los aquellos principios.

Para dar respuesta a los interrogantes surgidos es necesario que la medida supere inicialmente los cánones de aplicación del principio de proporcionalidad desarrollados tanto por la doctrina

[81] STJUE de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12.

[82] Para Robert ALEXY(2001) los derechos fundamentales constituyen *mandatos de optimización.* En otros términos: que los bienes protegidos por ellos deben proyectarse en todas sus posibilidades jurídicas y fácticas de realización (*Teoría de los derechos fundamentales*, CEPC, Madrid, p.195).

[83] STJUE de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12.

del TJUE, como por la doctrina del TC[84], que implicará un triple examen[85] de idoneidad, de necesidad y de proporcionalidad *strictu sensu*[86].

Por su parte, la LECrim establece dos criterios alternativos para determinar el nivel de gravedad de los delitos:

El primero es el estándar material identificado por conductas típicas de particular y grave relevancia criminógena que incorporan particulares tasas de lesividad para bienes jurídicos individuales y colectivos.

El segundo es un criterio normativo-formal basado en la pena prevista para el delito de que se trate. Este sería el de tres años de prisión que abarca a la gran mayoría de los delitos.

La controversia se suscita en la medida en si el interés del Estado en castigar conductas infractoras resulta suficiente para justificar injerencias desproporcionadas en los derechos fundamentales consagrados en la Carta.

Para el alto Tribunal aquellas injerencias producidas por el Estado y calificadas como graves, solo se podrán acordar en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos cuya pena prevista sea superior a los 3 años de prisión de conformidad con lo establecido en el art. 579 LECrim.

En cambio, si la injerencia puede considerarse de naturaleza no grave, estará siempre justificada su adopción por el simple objetivo de prevenir, investigar, descubrir y perseguir delitos en general, aun cuando la pena sea inferior a los 3 años de prisión.

Por ende, debemos conocer la interpretación que realiza el Tribunal para saber cuándo la injerencia podrá ser considerada de carácter grave.

Serán injerencias no graves aquellas que no comprometan la intimidad de los sujetos intervenidos y, por lo tanto, esos datos podrán ser cedidos sin mayores cautelas que las previstas por el legislador, en el ámbito de la prevención, investigación, descubrimiento y persecución de cualquier delito. Nos referimos a la identificación a los titulares de las tarjetas SIM activadas durante un periodo de doce días con el número IMEI de un teléfono sustraído, el acceso a los

[84] El juicio de proporcionalidad está orientado a resolver conflictos entre derechos, intereses o valores en concurrencia sin necesidad de generar jerarquías en abstracto de los derechos, intereses o valores involucrados y por tanto, sin necesidad de prejuzgar su mayor o menor legitimidad, ni producir prohibiciones absolutas (Encarna ROCA TRIAS, *Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española*, XV Conferencia Trilateral 24-27 de octubre 2013, Roma, p. 2).

[85] Juicio de idoneidad, mediante el cual el acceso a los datos conservados se adecúe objetivamente a la causalidad de la medida, que no es otra que la identificación de la persona que sustrajo el teléfono móvil. Juicio de necesidad, entendido como la alternativa menos gravosa, siendo la medida menos lesiva para los derechos de los ciudadanos. Juicio de proporcionalidad *strictu sensu,* realizando una ponderación entre los intereses de la investigación (interés del Estado) y los intereses individuales (interés del titular del derecho fundamental).

[86] Luis María DIEZ- PICAZO aboga por la ponderación como técnica de aplicación de las normas sobre derechos fundamentales (*Sistema de derechos fundamentales*, 3ª edición, edit. Aranzadi, Pamplona, 2008, p. 445).

números de teléfono correspondientes a las tarjetas SIM así como datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y, en su caso, la dirección.

A la inversa, se consideran injerencias graves y, en consecuencia, solo se podrán acordar en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos cuya pena prevista sea superior a los 3 años de prisión de conformidad con lo establecido en el art. 579 LECrim las que permiten extraer conclusiones precisas sobre la vida privada de las personas. Lo serán el acceso a las comunicaciones efectuadas con el teléfono sustraído, la localización de este, el acceso a datos que permitan conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM, los lugares en que estas comunicaciones tuvieron lugar y la frecuencia de estas con determinadas personas durante un período concreto.[87]

8. Conclusiones

Tras la realización de este estudio surgen algunos aspectos básicos en torno a los cuales debemos realizar nuestras consideraciones finales.

La primera es el innegable acierto en la incorporación de la cesión de datos como medida contemplada en la LECrim a los fines de prevención e investigación de delitos. Asimismo, no será posible la construcción de una verdadera Europa de Justicia, Seguridad y Libertad, sin que el principio de disponibilidad de datos cobre toda su relevancia en los distintos ordenamientos jurídicos de los estados miembros. La utilidad de la diligencia, unida al imparable desarrollo tecnológico, hacen que se trate de una herramienta imprescindible en las investigaciones judiciales, así como en la política criminal preventiva no solo a nivel nacional, sino también comunitario.

No obstante, se trata de una diligencia controvertida que puede afectar injustificadamente a los derechos fundamentales de cualquier persona, con independencia de sus actos y circunstancias del tipo que fueren. Por este motivo, para que la adopción de la medida no se oponga a los derechos reconocidos en la CEDF, es necesario dar cumplimiento a los requisitos legalmente establecidos, así como a los pautas y orientaciones desarrolladas por la jurisprudencia del TJUE, en tres sentencias clave.

La segunda nota a considerar, es el alcance del principio de proporcionalidad cuya evolución jurisprudencial ha permitido establecer criterios claros y precisos para determinar el nivel de injerencia del acceso a los datos conservados por parte de la autoridad competente. Con ese objetivo, aquellos datos que no permitan extraer conclusiones precisas sobre la vida privada de las personas y no supongan una injerencia grave podrán ser utilizados en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos (con independencia de la pena que lleven aparejada). Por el contrario, aquellas injerencias graves sólo podrán llevarse a cabo el ámbito de la prevención, investigación, descubrimiento y persecución de delitos cuya pena prevista sea superior a los 3 años de prisión de conformidad con lo establecido en el art. 579 LECrim, debido a la considerable vulneración de los derechos fundamentales establecidos en la Carta.

[87] Conclusiones del Abogado General Sr. Henrik Saugmandsgaard presentadas el 3 de mayo, asunto C-207/16.

Otro de los asuntos que merecen una profunda reflexión es la divergencia entre los estándares de garantías fijados respecto a la transferencia transfronteriza de datos personales y el nivel garantista del derecho interno para su tratamiento dentro de su propio estado. En cuanto a la aplicación del derecho comunitario debemos prestar especial atención al estándar de protección de los derechos fundamentales, de conformidad con el contenido de la Carta (arts. 7 y 8), así como la jurisprudencia que la interpreta. Afirmada la competencia del derecho nacional, la protección de los derechos fundamentales la orientaremos a la LECrim, interpretada a la luz del art. 18 CE y a la jurisprudencia constitucional.

Podemos constatar que el estándar de protección de los derechos fundamentales es de mayor intensidad en el derecho interno que en el Derecho comunitario. En consecuencia, si realizamos una interpretación amplia de cuándo es aplicable el Derecho de la Unión, estaremos rebajando el nivel de protección de los derechos fundamentales, en perjuicio del ejercicio de los mismos. El efecto que se desprende de la situación descrita es una mayor facilidad en la persecución de la delincuencia y en definitiva, de la actuación del derecho. Por el contrario, si damos prevalencia al derecho interno, admitiendo menor protección de los derechos fundamentales, podría suponer un reclamo delictivo al entender los infractores que las garantías procesales son obstáculos que impiden la investigación de delitos y a la postre, la aplicación del *ius puniendi* del Estado.

Ante este panorama expuesto se evidencia la necesidad de armonización de las legislaciones nacionales de los Estados miembros en materia de derechos fundamentales, cuyos estándares de protección sean equivalentes. A la espera de un verdadero código procesal europeo deberemos incorporar a los respectivos ordenamientos jurídicos las interpretaciones realizadas por el Alto Tribunal con motivo de las distintas cuestiones que se vayan planteando.

9. Bibliografía

Teresa ARMENTA DEU (2017), *Lecciones de derecho procesal*, edit. Marcial Pons, 10ª edición, Madrid.

- "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, whatsapp, redes sociales): entre la insuficiencia y la incertidumbre."

Robert ALEXY (2001), *Teoría de los derechos fundamentales*, CEPC, Madrid.

Nicolás CABEZUDO RODRIGUEZ (2018), *Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal*, BMJ núm. 2186.

Julio BANACLOCHE PALAO y Jesús ZARZALEJOS NIETO (2015), *Aspectos fundamentales del Derecho procesal penal*, La Ley, Madrid.

Federico BUENO DE MATA (2019), Las diligencias de investigación penal en la cuarta revolución industrial, Edit. Aranzadi, Navarra.

Raquel CASTILLEJO MANZANARES (2010), *Hacia un nuevo proceso pena*l, La Ley, Madrid.

Ignacio COLOMER HERNÄNDEZ (Dir.) y Sabela OUBIÑA BARBOLLA, S. (Coord.) (2015), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Edit. Aranzadi, Cizur Menor:

- ELS DEL BUSSER, *La creciente involucración de las empresas privadas en las investigaciones penales de la UE*.
- Alfonso GALÁN MUÑOZ, *La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea.*

Jesús CONDE FUENTES. Y Gregorio SERRANO HOYO (2019), *La justicia digital en España y la Unión Europea*, edit. Atelier, Barcelona:

- Raquel BONACHERA VILLEGAS, *La protección de datos de carácter personal en el ámbito judicial.*
- Paloma ARRABAL PLATERO, *Algunas cuestiones controvertidas sobre la obtención de datos de tráfico.*

Luis María DIEZ PICAZO (2008), *Sistema de derechos fundamentales*, 3ª edición, edit. Aranzadi, Pamplona.

Fernando GASCÓN INCHAUSTI (2012), *Investigación transfronteriza, obtención de prueba penal en el extranjero y derechos fundamentales (Reflexiones a la luz de la jurisprudencia español)*, Derecho Procesal Español del S. XX a golpe de tango, Tirant lo Blanch.

Isabel GONZALEZ CANO (2018), *Derecho y Proceso, Liber Amicorum Vol.II*, edit. Atelier, Libros jurídicos, Barcelona.

Nicolás GONZÁLEZ CUELLAR SERRANO (2013), *Problemas actuales de la Justicia Penal*, Colex, Madrid:

- Paloma ARRABAL PLATERO, *Algunas cuestiones controvertidas sobre la obtención de datos de tráfico.*
- Vicente GIMENO SENDRA, *La prueba preconstituida de la policía judicial*.

María Fuensanta GÓMEZ MANRESA. Y Manuel FERNÁNDEZ SALMERÓN (2019), Modernización digital e innovación en la Administración de Justicia, edit. Aranzadi.

Fernando JIMENEZ CONDE Y Rafael BELLIDO PENADES (2019), *Justicia: ¿Garantías versus Eficiencia?* edit. Tirant lo Blanch, Valencia:

- Julio PEREZ GIL, *Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal.*

Araceli MANGAS MARTÍN (2008), *Artículo 51. Ámbito de aplicación* en *Carta de los derechos fundamentales de la Unión Europea. Comentario artículo por artículo*, edit. Fundación BBVA.

Elena MARTINEZ GARCÍA (2016), *La orden europea de investigación. Actos de investigación, Ilicitud de la prueba y cooperación judicial transfronteriza*, edit. Tirant lo Blanch, Valencia.

Juan MONTERO AROCA (2012*), El derecho procesal español del siglo XX a golpe de tango*, *Liber Amicorum* en homenaje y para celebrar su LXX cumpleaños, edit. Tirant lo Blanch, Valencia.

Pablo NUEVO LÓPEZ (2015), *Control de convencionalidad y aplicación judicial de los derechos fundamentales de la Unión Europea*, Revista de Dret Públic, nº 50.

José Luis RODRIGUEZ LAINZ (2014), *Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la Ley española sobre la conservación de datos relativos a las comunicaciones*, Diario La Ley, nº8308, Sección doctrina, 12 de mayo 2014, Ref. D-148, Editorial LA LEY.

- *Intervención judicial en los datos de tráfico de telecomunicaciones electrónicas*, Bosch, Barcelona, 2003.

Encarna ROCA TRIAS (2013), *Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española*, XV Conferencia Trilateral 24-27 de octubre 2013, Roma.

María Isabel ROMERO PRADAS, *La prueba penal en Europa, una cuestión compleja: La orden europea de investigación como nuevo instrumento de obtención de pruebas en procesos penales trasnacionales y su próxima incorporación al derecho español*, en *Integración Europea y Justicia Penal*, coord. María Iabel GONZÁLEZ CANO, 2018.

Andrés SAÉNZ DE SANTAMARÍA, Ignacio GONZÁEZ VEGA Y Bernardo FERNÁNDEZ PÉREZ (1999), Introducción al Derecho de la Unión Europea, Edit. Eurolex, Madrid.

Pilar SOLAR CALVO (2012), *La doble vía europea en protección de datos*, la Ley, nº 2832.

Francisco SOTO NIETO (2005), *Fundamentos constitucionales del derecho penal europeo*, Revista General del Derecho Penal, núm. 3.

Claudia WARKEN, *Classification of Electronic Data for Criminal Law Purposes*, Eu Crim 2018/4 (http://doi.org/10.30709/eucrim-2018-023/).