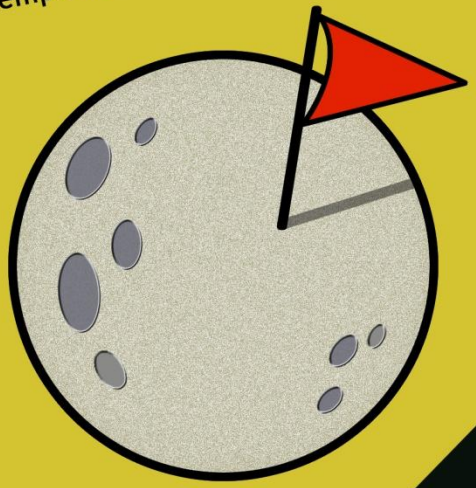
CYBERLAW by CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

Em pleno século XXI, o ciberespaço assume-se como o novo plano da acção. Este, representa, entre outras dimensões, um conjunto cada vez mais alargado e eficiente de meios de comunicação e de informação ao serviço do Homem. A sociedade hodierna, inebriada por esta revolução tecnológica, numa quase-metamorfose híbrida, adapta-se a esta tecno-dependência. Mas, será que compreendemos, minimamente, o advento do ciberespaço e do tempo moderno em que vivemos?



CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

CYBERLAW by CIJIC

CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 01 janeiro 2016 | Grátis

DIREITO: A PENSAR TECNOLOGICAMENTE

cyber espaço
novas fronteiras

cyber ataques
algumas estratégias de mitigação

cyber segurança
preocupação global

outros
- direito constitucional do Inimigo
- obscurantismo
- DOTMLPI-I
- ENISA


CYBERLAW
by CIJIC

CYBERLAW
by CIJIC

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

THE PROTECTION OF PERSONAL DATA IN PROCESSINGS INTENDED TO THE PREVENTION, INVESTIGATION AND PUNISHMENT OF CRIMES: IN DIRECTION TO A NEW DIRECTION OF THE EUROPEAN UNION'S CRIMINAL POLICY

ALFONSO GALAN MUÑOZ [1]

[1] Profesor Titular de Derecho Penal Universidad Pablo de Olavide de Sevilla/España. Correo electrónico: agalmun@upo.es
Este trabajo se ha realizado en el marco del Proyecto del Ministerio de Ciencia e Innovación I+D+I, titulados "La transmisión de datos personales en la copelación policial y judicial penal en la Unión Europea: el Principio de Disponibilidad" (DER 2011/28282) y del Proyecto Investigación I+D del Ministerio de Economía y Competitividad sobre "Cesión de datos personales entre procesos penales y procedimientos administrativos o tributarios en España y la Unión Europea" (DER2014-56401-P).

RESUMO

Este artigo procura analisar as diferentes etapas temporais da política penal estabelecida pela União Europeia relativas ao processamento de dados pessoais usados na prevenção, investigação e punição de crimes, até chegarmos à situação presente. Uma situação em que a União deverá repensar a sua política procurando adoptar uma muito mais incisiva na protecção dos direitos fundamentais das pessoas, em especial no tocante ao direito fundamental à protecção de dados pessoais, isto se pretender responder adequadamente às exigências do novo quadro normativo criado pela adopção e entrada em vigor do Tratado de Lisboa e à interpretação do Tratado que o Tribunal de Justiça Europeu tem vindo a seguir em algumas das suas últimas sentenças.

Palavras-Chave: Direitos fundamentais; Dados pessoais; Dados de tráfego; Direito penal europeu; Cooperação policial e judiciária.

ABSTRACT

This paper analyses the different stages of criminal policy established by the European Union in relation with personal data processing that is used to prevent, investigate and punish crimes, until come to the current situation. The situation in which the Organisation must rethink its policy in order to take one policy much more pointed to protect the fundamental rights of people and, especially, the fundamental right of personal data protection, if it wants answer adequately to the demands of the new normative frame created by the adoption and entry into force of the Treaty of Lisbon and the interpretation of this Treaty that the European Court of Justice has done in some of its last sentences.

Keywords: Fundamental rights, personal data, traffic data, European Criminal law, police and judicial cooperation.

RESUMEN

El presente trabajo analiza las diferentes etapas que ha atravesado la política criminal seguida por la Unión europea en relación con los tratamientos de datos personales utilizados para prevenir, investigar o sancionar delitos, hasta llegar a la situación actual. Una situación en la que dicha institución tendrá que replantearse la mencionada política, adoptando una mucho más orientada a la protección de los derechos fundamentales de las personas y, especialmente, del derecho fundamental a la protección de datos personales, que la ha seguido hasta este momento, si realmente pretende responder, de forma adecuada, a las exigencias que se derivan del nuevo marco normativo que la aprobación y entrada en vigor del Tratado de Lisboa ha venido a establecer y a la interpretación que del mismo ha efectuado el Tribunal Europeo de Justicia en alguna de sus últimas sentencias.

Palabras claves: Derechos fundamentales, datos personales, datos de tráfico, Derecho penal europeo, cooperación policial y judicial.

1.EL LARGO CAMINO DEL DERECHO PENAL EUROPEO Y SU INCIDENCIA EN LA REGULACIÓN DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Uno de los fenómenos más interesantes y relevantes que se han producido en el Derecho penal de estos últimos años se ha derivado del lento, pero imparable nacimiento de lo que ya podemos considerar como un verdadero Derecho penal europeo.

Parecen ya lejanos los días en los que la doctrina discutía sobre el concreto origen del *ius puniendi* positivo de la Unión europea, cuestionando, por ejemplo, si fue el reconocimiento el principio de asimilación en algunas Sentencias Comunitarias, como la referida al asunto del Maíz Griego, el que supuso la aparición de dicha capacidad normativa[2]; o si fueron, en realidad, las posteriores Sentencias del mismo Tribunal que reconocieron la legitimidad de las instituciones comunitarias, y especialmente las de la Comisión, a la hora de emitir normativa sobre las cuestiones penales en las que dicha regulación resultase necesaria para hacer un uso efectivo y adecuado de las competencias que les correspondían en materia de integración, las que realmente dieron lugar a su nacimiento[3].

Lo cierto es que la UE ha ido creando, a lo largo de los últimos años, una ingente normativa en materia penal, cuya aparición ha dado lugar a que se pongan en tela de juicio, tanto la base competencial sobre la que se ha regulado tal materia, como la más

[2] Sentencia del TJCE 28/88, de 2 de septiembre de 1989.

[3] Véase, en especial, lo establecido en la sentencias del TJCE de 13 de septiembre de 2005 y en la de 23 de octubre de 2007. Sobre todo el proceso jurisprudencial que llevó hasta el reconocimiento de dicha capacidad normativa, véase, por ejemplo, lo comentado por FERNÁNDEZ OGALLAR, B. en *El Derecho penal armonizado de la Unión europea.* Ed. Dykinson. Madrid, 2014. p. 183 y ss. Hay que destacar, por otra parte, que mientras algunos autores, como TIEDEMANN, K., hablaban de la existencia de un mero Derecho penal nacional europeizado, precisamente, por entender que, al fin y al cabo, por más que la Unión europea pudiese emitir normativa con contenido penal, la misma no sería vinculante hasta que no fuese transpuesta a cada uno de los ordenamientos jurídicos nacionales de sus Estados miembros por cada uno de sus respectivos paramentos. «EG und EU als Rechtquellen des Strafrechts» en *Festschrift für Claus Roxin.* V Walter Gruyter. Berlín. Nueva York, 2001. p. 1430; otros, como VOGEL, J. señalan, más acertadamente, a nuestro modo de ver, que, dado el carácter vinculante de la normativa comunitaria para los Estados y sus parlamentos y la cada vez más detallada regulación de los contenidos penales sobre la que la misma recaía, la intervención de los parlamentos nacionales terminaba convirtiéndose, en realidad, en una mera salvaguarda formal del principio de legalidad, ya que dichos parlamentos se veían de hecho obligados a acatar y ejecutar las decisiones de política criminal adoptadas desde Bruselas. En «Política criminal y dogmática penal europea», en RP núm. 11, 2003, pp. 143 y 144. En este mismo sentido, SCHÜNEMANN, B. llegó incluso a afirmar que los parlamentos nacionales habían terminado por convertirse en meros «lacayos de Bruselas», en «Fortschritte und Fehltritte in der Strafrechtspflege der EU», en *GA*, 2004. pp. 194 y ss.

que discutible legitimación democrática que ampararía su emisión; críticas que muy posiblemente hayan sido las que han llevado a que el, por el momento, último gran paso dado en el proceso de construcción de la Unión Europea, el Tratado de Lisboa, suscrito el 13 de diciembre de 2007, haya tratado de afrontar ambos problemas realizando dos grandes aportaciones con respecto a los mismos.

La primera consistió en reconocer, de forma expresa, que la Unión tenía competencias tanto en materia de Derecho penal sustantivo, —materia en la que podrá crear normas mínimas que definan las infracciones penales y sanciones que resulte necesario establecer para desarrollar de forma efectiva las políticas de armonización propias de la Unión (artículo 83.2 TFUE) o las que se refieran a ámbitos criminales dotados de especial gravedad y dimensión transfronteriza, como el terrorismo, la criminalidad organizada, el tráfico de drogas, el blanqueo o la criminalidad informática, entre otros (artículo 83.1 TFUE)—, como en relación a cuestiones de naturaleza procesal penal (artículo 82 TFUE) o incluso en las de pura prevención de delitos (artículo 84 TFUE)[4]. La segunda, por su parte, se derivó del hecho de que el citado Tratado estableciese que todo este proceso de armonización legislativa en materia penal se habría de realizar utilizando el procedimiento normativo ordinario, lo que llevará a que todas las disposiciones que lo desarrollen se tengan que adoptar a través de un proceso de codecisión en el que el Parlamento europeo, único órgano europeo dotado de legitimidad democrática directa, asumirá un papel, tal vez no suficiente, pero sí mucho más relevante que el que hasta ese momento había tenido, en el proceso de creación de dicha normativa[5].

No parece, pese a todo, que éste vaya a ser el último gran paso que se dé en este constante y aparentemente imparable camino hacia el desarrollo de un verdadero y esperemos que, en un futuro cercano, plenamente legítimo Derecho penal europeo[6], y

[4] Precisamente, y a juicio de VOGEL, J. esta última es una de las más evidentes ampliaciones de competencias que la entrada en vigor del Tratado de Lisboa ha traído con consigo a la UE, junto al hecho de que prevea la colaboración entre administraciones no específicamente referidas a la justicia y a las decisiones que se emitan desde estas últimas, por más que no estén referidas a materia penal. En «EU-Arbeitsweisevertrag Artikel 82 Gegenseitige Anerkennung; Angleichung», en *Das Recht der Europäischen Union.* 51 Ergänzungslieferung, V. Becks, München, 2013, Rnd. 66. sobre la cuestionada posibilidad de la existencia de otras bases competenciales de la UE en materia penal, véase, por ejemplo, lo comentado por MAPELLI MARCHENA, C., *El modelo penal de la Unión europea*. Ed. Aranzadi, Cizur Menor, 2014, pp. 160 y ss.

[5] FERNÁNDEZ OGALLAR, B., op. cit. ant., pp. 74, 133 y ss. y 349 y ss.

[6] Sobre los problemas de legitimidad que enfrenta este Derecho, véase, de forma general, lo comentado por ejemplo, por FERNÁNDEZ OGALLAR, B. en op. cit. ant., pp. 349 y ss. Resulta destacable en este aspecto, que mientras algunos autores como. NIETO MARTÍN, A. se mostraban favorables a

hacia la paralela implantación una auténtica política criminal europea, que permita, entre otras cosas, que tanto los organismos nacionales, como los europeos responsables de la prevención, persecución y sanción de delitos cuenten con los medios que realmente necesitan para poder ejercer sus competencias, de forma efectiva, en el mundo globalizado y carente de fronteras en el que vivimos[7].

Precisamente, una de las principales herramientas y medios de los que todos estos organismos deben disponer para cumplir con sus funciones, es, sin lugar a dudas, la información. Cuanto más información y de mayor de calidad tengan los agentes responsables de la prevención, la investigación o la represión de delitos, más eficazmente desempeñarán su labor, lo que debería llevar a la UE a crear y establecer los instrumentos materiales y normativos necesarios para permitir que dichos agentes puedan obtener e intercambiar entre sí los datos que necesiten, de la forma más rápida y fiable posible.

Ahora bien, no todo puede reducirse a conseguir la mayor eficacia preventiva y represiva. Si la Unión Europea realmente pretende ser ese espacio único, no solo de Seguridad, sino también de Libertad y Justicia del que habla el artículo 67 su Tratado de Funcionamiento (TFUE), tendrá que tener presente que, junto a la búsqueda de las comentadas finalidades preventivas y represivas y, en la otra parte de la balanza, siempre habrá de encontrarse el respeto y la garantía de los derechos fundamentales de los ciudadanos, lo que, en el concreto caso que nos ocupa, obliga a que toda

---

considerar que el proceso de codecisión podría cumplir con las exigencias derivadas del principio de legalidad, si garantiza la intervención del Parlamento europeo y dejar margen a los nacionales para determinar la concreta transposición de la normativa europea, en «Posibilidades y límites de la armonización del Derecho penal nacional tras Comisión v. Consejo. (Comentario a la STJCE, asunto C-176/03, de 13-9-2005)». *REDE* núm. 17, 2006. p. 119, mientras que GÓMEZ-JARA DÍEZ, C. afirmaba incluso que el camino emprendido con el establecimiento de dicho proceso, podría tender a crear un Derecho penal europeo de corte federalista, en «Constitución europea y Derecho penal: ¿Hacia un Derecho penal Federal europeo?», en *Derecho penal y política transnacional*, Ed. Alitier, Barcelona, 2005. pp. 168 y ss. Otros, como SILVA SÁNCHEZ, J. M., por su parte, se han mostrado tremendamente críticos con la legitimidad democrática que aporta el proceso de codecisión implantado, en «Los principios inspiradores de las propuestas de un Derecho penal europeo. Una aproximación Crítica», *RP* núm. 13, 2004, pp. 145 y ss. o han considerado, como hace VOGEL, J. que dicho proceso debería ser mejorado ya que entre otras cosas y por ejemplo, debería permitir que el Parlamento goce de iniciativa legislativa, en «Política criminal y dogmática penal europea», en *RP* núm. 11, 2003, p. 144.

[7] Así, señalaba VOGEL, J. que la cooperación moderna no puede quedar reducida a la faceta de represión de delitos, sino que tiene que tener en cuenta aspectos de investigación proactiva y de prevención del crimen, lo que ha de ser muy tenido en cuenta a la hora de regular la cooperación policial, pero también al hacerlo con la judicial, ya que de no hacerse, dará lugar a importantes problemas de coordinación a la hora de, por ejemplo, transferir y utilizar las pruebas obtenidas durante la realización de la labor policial al correspondiente procedimiento judicial. En «Cooperación penal: cinco tendencias. Cinco propuestas para una acción futura», en *El Derecho penal de la Unión europea. Situación actual y perspectivas de futuro.* Ed. UCLM. Cuenca, 2007, pp. 161 y 162.

captación, transferencia o tratamiento de información que se efectúe en aras a prevenir o reprimir delitos, tenga que partir del más estricto respeto a ese derecho fundamental de nuevo cuño que se ha venido a denominar como derecho fundamental a la protección de datos de carácter personal[8].

La normativa creada por la UE para regular esta compleja cuestión ha sido profusa y variada y su paulatina y sucesiva aprobación ha dado lugar a una confusa y aparentemente no del todo coordinada regulación, cuyo concreto contenido ha respondido, como no podía ser de otra forma, a las diferentes fases que la política criminal europea ha ido viviendo hasta llegar al momento actual.

Veamos ahora, aunque sea de forma somera, cuáles han sido los principales hitos que han ido jalonando este largo y complejo proceso normativo.

[8] El nacimiento y la progresiva autonomización de este derecho fundamental con respecto al de la intimidad están íntimamente ligados con el proceso de delimitación que de ambos derechos ha ido realizando nuestro Tribunal constitucional. Así, fue este tribunal el que señaló, inicialmente, en su STC 254/1993, de 20 de julio, que, pese a que el artículo 18.4 CE protege expresamente derechos como la intimidad o el honor, con lo que actúa como instituto de garantía de los mismos, realiza dicha labor otorgando a la persona un haz de facultades positivas de control sobre todos sus datos que trascienden a los que tradicionalmente definen a dichos derechos fundamentales, lo que demostraría, a su juicio, que tal precepto constitucional establecía un nuevo derecho o libertad fundamental autónomo, aunque conectado con aquellos, que podría quedar encuadrado bajo el nuevo y más amplio concepto de la privacidad. Sin embargo, y unos años más tarde, fue el mismo tribunal el que desarrollando dichos argumentos, afirmó, en su decisiva STC 292/2000, de 30 de noviembre, que, en realidad, el derecho contemplado en el artículo 18.4 CE otorgaba a las personas un poder de control sobre sus datos de carácter personal, tanto privados como públicos, que le convertía en titular de unas facultades positivas que imponían a terceros deberes jurídicos, (como los de informar, pedir el consentimiento, permitir el acceso, rectificar o cancelar los datos, etc.), y que no solo trataban de proteger su intimidad, sino que también tutelaban a todos los bienes de la personalidad que pertenecían a su vida privada y estaban unidos a su dignidad personal, lo que convertiría a la protección de dichos datos en un derecho fundamental independiente y diferente de la intimidad y también de la privacidad, ya que, de hecho, le otorgaba a su titular unas facultades y unos poderes que trascendían con mucho a los que definían a estos dos últimos derechos. Se independizaba así este derecho del derecho a la intimidad, incluso entendido en su más moderna y amplia concepción que abarcaría al denominado derecho a la autodeterminación informativa, lo que nos ha llevado a considerar al derecho a la protección de datos de carácter personal como un verdadero derecho fundamental diferente y completamente autónomo de la intimidad, pese a lo aún hoy mantiene una parte de nuestra doctrina. Véase a este respecto lo sostenido, por ejemplo, por GUICHOT, E., *Datos personales y administración pública*, Ed. Aranzadi, Cizur Menor (Navarra) 2005, 108 y ss. y los argumentos que, frente a la postura finalmente sostenida por este autor, mantuve en GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación», en *Revista General de Derecho penal*, núm. 19, 2013, pp. 4 y ss., en <http://www.iustel.com/> (últ. vis. 20-4-2014).

2.EL PRINCIPIO DE DISPONIBILIDAD COMO REFERENTE INICIAL DE LA POLÍTICA CRIMINAL EUROPEA RELATIVA A LA COOPERACIÓN JUDICIAL Y POLICIAL EN MATERIA INFORMATIVA.

La Unión europea tomó pronto conciencia de la importancia que los tratamientos de datos iban a tener para el tráfico económico del mercado único. Por ello, ya en el año 1995 emitió la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, (más conocida como Directiva General de Protección de datos personales)[9], cuya aprobación dio lugar, entre otras cosas, a la reforma que, sobre la legislación española referida a esta materia, realizó la todavía vigente Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[10].

Pese a la amplitud que caracterizó a la referida norma comunitaria, pronto se hizo evidente que la misma no iba a poder responder a todos los retos y particularidades que planteaba la aparición y rápida expansión de las nuevas tecnologías de la información y la comunicación y, en especial, a los que generaba Internet.

Por ello, tan solo dos años después de la aprobación de dicha Directiva, el regulador comunitario se vio obligado a aprobar otra, la Directiva 97/55/CE, de 15 de diciembre, precisamente referida al tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones; normativa que, pese a todo, solo 5 años más tarde tuvo que volver que ser actualizada, mediante su sustitución por la aún vigente Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de datos

[9] Así, señala PARIENTE DE PRADA, I. que dicha Directiva se aprobó en un contexto caracterizado, precisamente, por el denodado esfuerzo de la Comisión europea por acabar con las trabas que limitaban el mercado único comunitario, lo que llevó a que dicha norma se desarrollase al amparo del artículo 100 del Tratado de la Comunidad Económica Europea en aquel momento vigente. En «La reforma de la protección de datos en el ámbito europeo», en *El Espacio de libertad, Seguridad y justicia: Schengen y protección de datos.* Ed. Azanzadi. Cizur Menor, 2013, pp. 127 y ss.

[10] En concreto, fue precisamente la transposición de la comentada Directiva la que obligó a reformar la primera legislación nacional específicamente reguladora de esta materia (la ya citada LOTADP), dando lugar a la aprobación de la todavía vigente Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPDP), que, entre otras muchas cosas, extendió la especial protección jurídica que se otorgaba a tales datos, no solo a aquellos que estaban recogidos en forma informática, como hacía la LOTAD, sino también a todos aquellos que se encontrasen en cualquier clase de soportes o ficheros que resultasen adecuados o idóneos para ser tratados, como exigía el artículo 2 de la Directiva 1995/46/CE.

personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[11].

Ya las propias denominaciones de las citadas normas comunitarias parecían indicar que no se habían creado para regular los tratamientos de datos de los que nos vamos a ocupar en este trabajo, esto es, los realizados para prevenir, investigar y reprimir delitos; impresión que se vio completamente ratificada por el hecho de que tanto el artículo 3.2 de la Directiva General de Protección de Datos Personales (la 95/46/CE), como el artículo 1.3 de la vigente Directiva 2002/58/CE, referida al sector de las telecomunicaciones, excluyesen de sus correspondientes ámbitos de aplicación precisamente a los tratamientos *«… que tengan por objetivo 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****»*.

Se optó así, claramente por mantener una doble vía a la hora de proteger los datos de carácter personal. Una general y garantista, en la que se reconocía al titular de dichos datos el control sobre los mismos, que, entre otras cosas y en principio, no podían ser recogidos, procesados, ni transmitidos sin contar con su consentimiento[12] y sobre los cuales conservaba unos derechos positivos de información, acceso, rectificación, cancelación y oposición (derechos ARCO), cuyo respeto debía ser controlado y garantizado por determinados organismos administrativos independientes expresamente dedicados a asegurar su efectividad; y una segunda, especial o excepcional, que quedaba al margen de dicha regulación general y de sus garantías, precisamente por entenderse que los tratamientos a los que estaba referida no podrían cumplir con los fines para los que se realizarían (la prevención, investigación y represión de delitos) si el titular de los datos sobre los que recayesen

[11] Sobre la evolución de esta normativa y los problemas a los que se enfrentaba en la moderna sociedad de la información, véase, por ejemplo, RODRÍGUEZ LAINZ, J. L., «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: Derecho derivado», en *LA LEY* núm. 7373, 2010 en <www.laley.es> (últ. vis. 12-4-2014).

[12] Debe señalarse, sin embargo, que los niveles de exigencia de dicho consentimiento varían, atendiendo, entre otras cosas, a la relevancia o especial sensibilidad de los datos de lo que se trate. Véase, por ejemplo y en relación a esta cuestión, lo señalado por APARICIO SALOM, J., *Estudio sobre la protección de datos*. Ed. Aranzadi, Cizur Menor, 2013, pp. 65 y ss. y 149 y ss. o SANTOS GARCÍA, D., *Nociones generales de la Ley orgánica de protección de datos y su reglamento: adaptado al RD 1.720/2007 de 21 de diciembre*. Ed. Tecnos, 2012, pp. 67 y ss., entre otros.

(p. ej. un sospechoso) conservase sobre los mismos todos los derechos que la normativa general le otorgaba[13].

Podría pensarse entonces, que la Unión europea se había mantenido inicialmente al margen de cualquier planteamiento que tuviese que ver con la articulación o armonización de esta segunda vía, de la estrictamente penal, habiéndose limitado a regular la primera por ser la que más clara y directamente incidiría en la libre circulación de mercancías, servicios y capitales que debía caracterizar el mercado único que dicha organización supranacional trataba de implantar y garantizar.

Nada más lejos, sin embargo, de la realidad.

La verdad es que los organismos comunitarios fueron pronto conscientes de que, desde el mismo momento en que se estableciese un espacio o mercado único de libre circulación de personas, capitales y mercancías, como el que en 1985 generó la ratificación y entrada en vigor del Acuerdo Schengen, se hacía necesario implementar medidas de coordinación y de información entre las distintas policías que iban a encargarse de controlar y asegurar la nueva frontera única y común que iban a tener todos los Estados integrados en tal espacio, lo que llevó a que, ya el 19 de julio de 1990 y dentro del Convenio de aplicación del Acuerdo Schengen, se crease y regulase un complejo sistema de intercambio de datos relativos a la identidad de las personas y la descripción de objetos buscados [el Sistema de Información Schengen (SIS)] que trataba, precisamente, de fomentar y facilitar la colaboración entre las autoridades

[13] La existencia de esta doble vía para la protección de datos personales es algo común en todos los ordenamientos jurídicos de los Estados miembros de la Unión Europea y así, en concreto, la propia LOPD española establece en su artículo 2.2.c) que su régimen de protección no será aplicable *«… a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada»;* mientras que su artículos 22, de forma mucho más general, reconoce expresamente que los cuerpos y fuerzas de Seguridad del Estado pueden recoger y tratar los datos de una persona sin contar con su consentimiento, si ello resulta necesario *«… para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales»* y su 23 otorga al responsable del fichero creado con tales fines, la potestad de denegar los derechos ARCO que corresponderían a los titulares de los datos que hubiese recopilado, si su ejercicio pusiese en peligro la seguridad pública o alguna investigación que se estuviese realizando. Sobre estas prescripciones y su incidencia, véase lo comentado por SOLAR CLAVO, P. «La doble vía europea en protección de datos», en *LA LEY* núm. 2832, 2012, en <www.laley.es> (últ. vis. 10-4-2014). En esta misma línea señala, por ejemplo, RODRÍGUEZ LAINZ J.L. en relación con el sistema de captación de datos referidos a las comunicaciones establecido por la Ley Española (Ley 25/2007) que traspuso a nuestro ordenamiento la Directiva 2006/24/CE, que la exención que contempla dicha ley con respecto al principio de consentimiento y la que permite a los proveedores no cumplir con los deberes generales de acceso y cancelación de datos de carácter personal que generalmente les correspondería a su titular, se han establecido, precisamente, para garantizar que los tratamientos que se realicen sobre dichos datos resultasen eficaces a efectos de la investigación y persecución de delitos. En «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», en LA LEY núm. 6859 y 6860, 2008, en <www.laley.es> (últ. vis. 12-2-2014).

policiales y aduaneras de dichos Estados, entre otras cosas, para luchar contra la criminalidad[14].

No fue éste, sin embargo, el único ni el último instrumento creado desde la Unión Europea con el fin de favorecer los intercambios de información y de datos de carácter personal entre las distintas administraciones que están, directa o indirectamente, llamadas a desarrollar labores de prevención o represión de delitos.

De hecho, no tardaron mucho en aparecer organismos como Europol[15] o sistemas, como el Sistema de Información Aduanero (SID)[16], que intentaban favorecer y facilitar al máximo el intercambio de información entre dichas administraciones de los Estados miembros para convertir al mercado único, también en un mercado seguro.

Ahora bien, si hay un momento decisivo en la creación y desarrollo de todos estos sistemas, éste es, sin duda, el que vino dado por la perpetración de los atentados terroristas producidos el 11 de septiembre de 2001 en Nueva York y, sobre todo, por los acaecidos el 11 de marzo de 2004 en Madrid y el 7 y el 21 de julio de 2005 en Londres[17].

No debe sorprender que, ante la magnitud y peculiares características de los referidos atentados, marcados, entre otras cosas, por la internacionalidad y descentralización de la organización terrorista que los perpetró, la Unión Europea optase por intensificar su programa de cooperación en materia penal fomentando y

---

[14] Sobre el nacimiento de este sistema, su funcionamiento y posterior transformación en el actual sistema de Información Schengen de segunda generación (SIS II) véase, lo comentado por RECUERO, P., «La protección de datos y Schengen: Una visión desde la experiencia española», en El Espacio de libertad, seguridad y justifica: Schengen y protección de Datos. Ed. Aranzadi. Cizur Menor, 2013, pp. 197 y ss.

[15] Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía, hecho en Bruselas el 26 de julio de 1995.

[16] Reglamento (CE) núm. 515/97 del Consejo de 13 de marzo de 1997 relativo a la asistencia mutua entre las autoridades administrativas de los Estados miembros y la colaboración entre éstas y la Comisión con objeto de asegurar la correcta aplicación de las legislaciones aduanera y agraria

[17] Sobre la incidencia de estos atentados en el desarrollo de esta normativa, véase lo comentado por FERNÁNDEZ, OGALLAR, B., op. cit. ant., p. 338 o AIXALA, A., quien diferencia, a su vez y dentro de este periodo, dos etapas distintas. Una primera que iría desde el atentando del 11 de septiembre en Nueva York hasta el del 11 de marzo en Madrid, donde, a su modo de ver, se adoptó un impulso primordialmente político a las medidas de cooperación judicial y policial, y otro que comenzaría con este último atentado, en el que se produjo un desarrollo mucho más técnico y, a su modo ver, también eficaz. En «La estrategia de la UE ante el terrorismo internacional y la defensa de los derechos y libertades», p. 51, en <http://www.iuee.eu/pdf-publicacio/1/jpjdqoe8lrscpmve8of8. Pdf> (últ. vis. 16-4-2014).

favoreciendo aún más el intercambio transfronterizo de información[18], llegando incluso el programa de trabajo establecido en la Haya, los días 4 y 5 de noviembre de 2004, a considerar, de forma expresa, como uno de los principales objetivos que la UE debería alcanzar, el de favorecer el intercambio de información entre los diferentes organismos nacionales y supranacionales llamados a desempeñar un papel en la prevención de este tipo de conductas.

Para lograrlo se crearon nuevos organismos, como Eurojust[19], y se multiplicaron los datos o ficheros específicamente destinados a favorecer la consecución de dichas finalidades, como los implantados conforme a lo dispuesto en la controvertida Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones,[20]. Pero además y por otra parte, se desarrolló e implantó un nuevo principio rector de la política criminal europea referida a esta clase de tratamientos de datos, el llamado «*principio de disponibilidad*», que tendería a garantizar que las autoridades de cualquier Estado de la UE tuviesen derecho a acceder y a disponer de las informaciones que necesitasen a efectos de prevenir, perseguir o sancionar delitos, cuando menos, en las mismas condiciones que podrían hacerlo las autoridades de

[18] Sobre este proceso y las sucesivas declaraciones emitidas en relación con esta materia, véase lo comentado por AIXALA, A., op. cit. ant. Entre estas declaraciones merece la pena destacar la emitida en Bruselas, el 25 de marzo de 2004, sobre la lucha contra el terrorismo por el Consejo tras el atentado de Madrid, donde se expresamente se afirmó que *«El Consejo Europeo, con el objeto de seguir desarrollando el marco legislativo mencionado más arriba, encarga al Consejo que estudie medidas en los siguientes sectores:*

- *propuestas destinadas a establecer normas sobre la conservación de datos de tráfico de comunicaciones por parte de los proveedores de servicios;*
- *intercambio de información sobre condenas por delitos de terrorismo;*
- *persecución transfronteriza;*
- *un registro europeo de condenas e inhabilitaciones;*
- *una base de datos sobre material forense, y*
- *simplificación del intercambio de información entre los cuerpos y fuerzas de seguridad de los Estados miembros».*

[19] Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

[20] Sobre el contenido de esta Directiva que modificó la previa Directiva 2002/58/CE y su transposición a nuestro ordenamiento véase, lo comentado, por ejemplo, por RODRÍGUEZ LAINZ, «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», cit. ant o GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas?…», cit. ant., pp. 46 y ss., entre otros.

aquel otro Estado miembro en el que la información en cuestión se encontrase registrada[21].

Este principio tuvo una enorme importancia normativa y quedó reflejado, por ejemplo, en la Decisión del Consejo 2008/633/JAI, de 23 de junio de 2008, que permitió a las autoridades responsables de la investigación y prevención de delitos de terrorismo y graves acceder al Sistema de Información de Visados (VIS), previamente creado por el Reglamento 767/2008, de 9 de julio, y también, en la Decisión Marco 2008/315/JAI , de 26 de febrero, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros, posteriormente desarrollada por la Decisión del Consejo 2009/616/JAI, de 6 de abril, que creó el Sistema Europeo de Antecedentes Penales (ECRIS), obligando a los Estados de los nacionales condenados penalmente en otro país, a recibir y almacenar los datos referidos a sus condenas, para poder ponerlos a la disposición de aquellos Estados miembros que se lo requiriesen[22].

Sin embargo, tal vez fuesen la Decisión 2008/615/JAI, del Consejo, de 23 de junio, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza[23], más conocida como la Decisión Prüm, por su por su estrecha relación con el Tratado firmado con anterioridad en dicha localidad alemana entre varios países miembros de la Unión[24], y la Decisión Marco 2006/960/JAI, del Consejo, de 18 de diciembre, sobre la

[21] VOGEL, J., «EU-Arbeitweisevertrag Artikel 82..»., cit. ant. Rnd. 70, ACED FÉLEZ, E., «Principio de disponibilidad y protección de datos en el ámbito policial» en <http://noticias.juridicas.com> (últ. vis. 11-3-2014).

[22] Sobre el proceso de consolidación del intercambio de antecedentes penales y el concreto funcionamiento del sistema ECRIS, véase, por ejemplo, lo comentado por BLANCO QUINTANA, M. J. en «La comunicación de antecedentes penales entre los Estados. El Sistema europeo de información de antecedentes penales», en *BMJ*, 2013, pp. 3 y ss.

[23] Desarrollada por la Decisión 2008/616/JAI del Consejo, de 23 de junio, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

[24] En concreto, el referido tratado internacional se firmó el 27 de mayo de 2005, en la Abadía benedictina de Prüm, entre el Reino de Bélgica, la Republica Federal de Alemania, España, Francia, Luxemburgo, Países Bajos y Austria, siendo posteriormente suscrito por Italia, Finlandia, Portugal y Eslovenia. De hecho, la aprobación de este tratado por parte de España es la que motivo la aprobación de la LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir de ADN, cuya entrada en vigor, como señala HOYOS SANCHO, M. ha llevado a que el sistema de transmisión de datos establecido por la comentada Decisión Marco se haya podido utilizar desde el inicio en España, sin necesidad de que el Consejo haya tenido que comprobar que nuestro ordenamiento había incorporado las disposiciones del capítulo 6 de dicha Decisión. En «Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos», en *Espacio europeo de libertad, seguridad y justicia: Últimos avances en cooperación judicial penal*. Ed. Lex Nova. Valladolid, 2010, p 164.

simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea[25], las normas europeas que dieron el mayor impulso a la implantación de dicho principio, 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.

Como se puede comprobar, el predominio de las políticas securitarias y represivas europeas durante este periodo fue, como era previsible, absoluto, quedando la garantía de los derechos a la intimidad y a la protección de datos personales de los ciudadanos en un muy segundo plano.

Así, mientras todas las normas comentadas tendían a facilitar al máximo la captación, el intercambio y el uso de información por parte de las autoridades implicadas en la investigación y represión de delitos, estableciendo, entre otras cosas, la obligación de los Estados miembros de tener disponibles los datos en cuestión y de entregarlos, incluso en plazos perentorios, a los organismos y autoridades competentes en dicha materia del resto de países de la UE[26], y reconociendo, incluso, la posibilidad de que la simple autorización del Estado cedente de los datos pudiese habilitar al cesionario para utilizarlos con fines diversos de aquellos para los que inicialmente los había solicitado[27]; sus textos dedicaron una prácticamente nula atención a la protección de los derechos y garantías que habrían de corresponder al titular de los datos personales tratados y transmitidos por tales sistemas, limitándose alguno a realizar alguna alusión general a la necesidad de que tales sistemas

[25] ACED FÉLEZ, E., op. cit. ant.

[26] Así, por ejemplo, y como señala ACED FÉLEZ, E. la Decisión Marco 2006/960/JAI, establece un plazo máximo de entrega de tan solo 8 horas en caso de urgencia, en op. cit. ant.; mientras que BLANCO QUINTANA, M. J. señala que las solicitudes de antecedentes penales realizadas por los Estados en relación a un procedimiento penal, utilizando el sistema ECRIS creado por la Decisión Marco 2009/315/JAI y la Decisión 2009/316/ JAI, deben ser atendidas en un periodo máximo de 10 días desde la recepción de la solicitud. En op. cit. ant., p. 22.

[27] Así lo hace, por ejemplo, el artículo 35 de la conocida como Decisión Prüm (la Decisión Marco 2008/615/JAI) que, como señala SAINZ HERMIDA, A., permite que los datos transmitidos puedan ser utilizados para otros fines, previa autorización de la Parte titular del fichero, siempre que tales fines estén previstos en el Derecho interno y la transmisión se realice de conformidad con el Derecho de la parte receptora, en «Protección de Datos…» cit. ant., p. 8. Algo más restrictiva es, pese a todo, la Decisión Marco 2009/315/JAI, cuyo artículo 9 establece que los antecedentes trasmitidos para su uso en un procedimiento penal solo podrán ser usados en aquel procedimiento para el que se solicitaron según consta en el impreso de solicitud, aunque su apartado tercero establece la excepción de que se podrán utilizar también *«…para evitar una amenaza inminente y grave para la seguridad pública».* Sobre este particular, véase lo comentado también por BLANCO QUINTANA, M. J., op. cit. ant., p. 23.

respetasen los derechos fundamentales reconocidos por el artículo 8 de la Convención Europea de Derechos Humanos (CEDH)[28], mientras que otros tan solo declaraban, en su parte expositiva y sin mayor precisión, que su articulado era, de hecho, conforme a lo establecido en la Carta de Derechos Fundamentales de la UE (CDFUE) y en especial, a los derechos a la intimidad y a la protección de datos de carácter personal que allí se contenían[29].

Puede que fuese esta situación la que llevó a que, más recientemente, el regulador europeo decidiese aprobar la Decisión Marco 2008/977/JAI, de 27 de noviembre, de protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, cuya creación, como indicaba su artículo 1, tenía por objetivo *«… garantizar* ***un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas*** *y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal, contemplada en el título VI del Tratado de la Unión Europea, garantizando al mismo tiempo un alto nivel de seguridad pública»*[30].

Pese a lo contundente de esta declaración, la verdad es que lo concretamente establecido en esta norma se presentó, ya desde un primer momento, como claramente insuficiente para conseguir tal fin.

No es sólo que, al haberse optado por establecer esta nueva normativa mediante la aprobación de una Decisión Marco, que, por definición, carecería de efecto directo sobre las normativas nacionales, se incrementase significativamente el riesgo de que se pudiesen dar importantes divergencias entre dichas regulaciones a la hora de transponer sus disposiciones, impidiéndose así que su aprobación pudiese servir para

---

[28] Así lo destaca RODRÍGUEZ LAINZ, J. L. con respecto a las Directivas 2002/58/CE y 2006/24/ CE viniendo el artículo 4 de la última Directiva citada, como señala el mismo autor, a determinar que el sistema de acceso a los datos que los proveedores tienen que almacenar para cumplir con lo en ella impuesto, debe atender a lo establecido en la CEDH. En «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas…», cit. ant.

[29] Así lo hace, por ejemplo, la conocida como Decisión Prüm (Decisión 2008/615/JAI del Consejo), cuyo considerando 18 del preámbulo parte precisamente parte del principio general de que la Decisión respeta dichos derechos.

[30] Precisamente, y con respecto a este precepto, destaca OERMANN, M. que mientras el artículo 8 de la CDFUE no aludía a ninguna finalidad a la hora de tutelar el derecho fundamental a la protección de datos, en el comentado precepto de la DM 2008/977/JAI se deja claro que su protección se pone en relación con de la seguridad pública, sin que el regulador haga establecido una prelación entre ambos fines. En OERMANN, M. *Individualdatenschutz im europäischen Danteschutzrecht*. V Centauros, Freiburg, 2012 p. 81.

alcanzar el deseable y necesario nivel de armonización en la materia que nos ocupa[31]; o que, al limitar paralelamente su ámbito de actuación a los intercambios transnacionales de datos realizados entre los Estados miembros, se dejasen al margen de su regulación y garantías a todos aquellos intercambios o tratamientos que se produjesen dentro de un único Estado, lo que podría dar lugar a la paradójica situación de que los titulares de datos que se incorporasen a los registros españoles mediante transferencias de otro Estado miembro pudiesen disfrutar de unos derechos y unas garantías de los que podrían carecer aquellos que vieron como sus datos se incluyeron en tales registros sin mediar dicha transferencia[32]; o incluso que, al no limitar su articulado suficientemente la finalidad con la que los Estados receptores podrían utilizar los datos que se les hubiesen transmitido, continuase dejando las puertas abiertas a que éstos puedan usarlos para fines completamente diferentes de los que fundamentaron su absolutamente excepcional captación y transmisión, esto es, para fines distintos de la mera persecución, investigación y represión de conductas penalmente relevantes[33].

Es que además y lo que es más importante, al no derogar ni modificar su articulado, lo que la multitud de normas comunitarias reguladoras de los diferentes sistemas de intercambio y facilitación de datos de carácter personal con fines penales establecen con respecto al funcionamiento y utilización de dichos sistemas, se convirtió a esta Decisión Marco en un instrumento que en nada afectó al verdadero «*patchwork*» normativo que existía ya en la UE con respecto a tales de tratamientos, con lo que se le dotó de una escasísima trascendencia práctica, quedándose muy lejos, por tanto, de alcanzar el objetivo para el que supuestamente se había creado, el de

[31] Así se deduce de lo establecido por el artículo 1 de la comentada Decisión Marco, como lo señala RODRÍGUEZ LAINZ, J. L., «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas…», cit. ant.

[32] ACED FÉLEZ, J., op. cit. ant. En este mismo sentido, SANZ HERMIDA, A. señala que se podrían dar divergencias en la protección otorgada a los datos que se transmiten, los internos y también con los que se podrían transmitir a terceros países a los que no les sea aplicable la normativa europea. «Protección de datos en la transmisión», cit. ant. p. 13.

[33] En este sentido, señala ALCAIDE FERNÁNDEZ, J. que los artículos 3 y 11 de esta Decisión Marco, también permiten que los datos inicialmente transmitidos para la realización de una investigación criminal puedan ser posteriormente utilizados para fines diferentes pero compatibles de los que justificaron dicha transmisión, afirmando, el referido autor que ello obligará a que tengan que ser los Estados los que deban determinar, en el ámbito nacional, de forma más precisa qué concretos fines posteriores se tendrán que considerar como incompatibles con el inicial, en op. cit. ant., p. 6.

establecer un alto nivel de protección para los derechos y libertades de las personas que se pudiesen ver afectadas por tales tratamientos[34].

El panorama, por tanto y como se puede comprobar, continuaría siendo, tras la aprobación de esta Decisión Marco, desalentador en lo que se refería a la protección de los derechos fundamentales de los ciudadanos. Sin embargo, tras este inicial y hasta cierto punto esperable comienzo, parecía que la aprobación y entrada en vigor del Tratado de Lisboa, suscrito por los Estados miembros de la Unión el 13 de diciembre de 2007, podría obligar a la UE a cambiarlo de forma radical.

3.UN NUEVO E IMPORTANTE REFERENTE NORMATIVO: EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA CDFUE TRAS LA ENTRADA EN VIGOR DEL TRATADO DE LISBOA

La aprobación y entrada en vigor del Tratado de Lisboa ha supuesto, entre otras cosas, que el nuevo artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) haya pasado a reconocer de forma expresa que toda persona tiene derecho a la protección de sus datos de carácter personal y que el Parlamento europeo tiene la obligación de establecer una normativa que garantice tal derecho[35].

Pero, además y lo que es incluso más importante para el tema que nos ocupa, también ha llevado a que el nuevo artículo 6 del propio Tratado de la Unión Europea (TUE) haya convertido, de una vez por todas, a la Carta de Derecho Fundamentales de la Unión Europea (CDFUE) en un instrumento de valor equivalente a los propios

[34] PEYROU, S., «Algunas reflexiones sobre la protección de datos en el ELSA o la crónica de una esperanza frustrada», en *El espacio de libertad, seguridad y justicia: Schengen y Protección de datos*. Ed. Aranzadi, Cizur Menor, 2013, p. 148, GONZÁLEZ MURUA, A. R., «El supervisor Europeo de protección de datos ante la revisión del marco jurídico de la protección de datos. Especial referencia a las reformas en el seno del espacio de libertad, seguridad y justicia», en *El espacio de libertad, seguridad y justicia: Schengen y Protección de datos*. Ed. Aranzadi, Cizur Menor, 2013, p. 246.

[35] En concreto, este precepto establece que: *«1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.* (…)», lo que llevó a TINNEFELD, M. T./ BUCHNER, B. /PETRI, T. a afirmar que dicho precepto deberá llevar a la unificación de la protección jurídica de datos en el nivel del Derecho derivado, atendiendo, eso sí, a los principios de subsidiaridad y proporcionalidad. En *Einführung in das Datenschutzsrecht.* V. Oldenburg, München, 2012. p. 136.

tratados constitutivos, lo que llevará a que sus prescripciones y derechos resulten directamente vinculantes para toda la Unión y para toda la normativa derivada que de ella proceda, dejando ya de actuar como un mero referente de esa serie de principios generales comunes a todos los Estado miembros que, según sostenía el Tribunal Europeo de Justicia, el Derecho de la UE debería tener en cuenta y tratar de respetar, para pasar a convertirse, por fin, en derechos plenamente vinculantes para dicha institución supranacional y su Derecho, con lo que su respeto se podrá exigir directamente ante el citado Tribunal[36].

Con ello, se reconoció expresamente la competencia de la UE para regular en materia de protección de datos personales y se introdujo, al mismo tiempo, la obligación jurídica de que todo el Derecho europeo derivado hubiese de respetar el derecho a la protección de dichos datos que se contiene en el artículo 8 de la CDFUE; precepto que, entre otras cosas y como señala OERMANN, a diferencia de lo que sucede, por ejemplo, con el artículo 3 de la todavía vigente Directiva General de Protección de Datos personales (la 95/46/CE), no contempla ninguna limitación expresa del ámbito de aplicación de este derecho en relación a las materias de policía, justicia o defensa de los Estados vinculados por tal tratado[37].

Parecía entonces, que el comentado Tratado tendía a adoptar un enfoque mucho más transversal y orientado hacia la protección de los datos de carácter personal que el que hasta aquel momento había mantenido la UE y, consecuentemente, obligaría a

---

[36] En concreto, el artículo 6 de TUE establece que *«La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados.*
Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados.
Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones. (…)». Sobre la trascendencia de dicha declaración normativa, véase lo comentado por FERNÁNDEZ, OGALLAR, B., op. cit. ant., pp. 53 y ss. y 72, mientras que sobre la situación previa a la entrada en vigor de este Tratado y el tratamiento que el Tribunal Europeo de Justicia dio a lo establecido tanto en el CDFUE o en el CEDH, resulta interesante la lectura de lo comentado por RODRÍGUEZ LAINZ, J. L en «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: Derecho primario», en *LA LEY*, núm. 7373, 2010, <www.laley.es> (últ. vis. 12-4-2014).

[37] OERMANN, M., op. cit. ant., p. 77. Ha de señalarse, en esta misma línea, que, como mantiene PEYROU, S., pese a que en un principio el nuevo artículo 16 del TFUE tampoco establezca excepción alguna en materia de policía o derecho penal a la necesidad de regular y garantizar dicho derecho, excepcionando del mismo tan solo las materias de extranjería y seguridad común, la Declaración núm. 21 aneja al Tratado de Lisboa sí que prevé expresamente la adopción de reglas específicas o excepciones en materia de cooperación judicial o policial en materia penal. Op. cit. ant., pp. 152 y 153.

dicha institución a revisar la regulación que hasta entonces había creado sobre la materia[38].

Así de hecho, se indicó en el Programa de Estocolmo (COM (2010) 171), que definió las orientaciones de la UE en el marco del Espacio de Libertad, Seguridad y Justicia para el periodo 2010-2014, y en la Agenda Digital para Europa (COM (2010) 245), en cuyo desarrollo, la Comisión europea elaboró e hizo público, el 25 de enero de 2012, un importante paquete normativo, tendente a establecer un nuevo marco normativo en materia de protección de datos de carácter personal, que estaría compuesto por dos normas fundamentales[39]: Una propuesta de Reglamento que vendría sustituir a la ya citada Directiva General de protección de datos personales[40] y una de Directiva llamada a reemplazar a la ya comentada y criticada Decisión Marco 2008/977/JAI, para establecer, como su propio título indica, un sistema de «*... protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos*»[41].

Con ello, y como fácilmente se puede deducir, se continuaba manteniendo la doble vía que había caracterizado a la regulación europea referida a la protección de datos personales hasta ese momento, diferenciando, una general, regulada en el proyectado Reglamento y una específica o excepcional, contenida en la propuesta de Directiva, que trataría de establecer un régimen especial que respondiese adecuadamente a las particulares necesidades que planteaba la cooperación informativa, policial y judicial, en materia penal[42].

Esta última regulación presentaría significativas y destacables diferencias con respecto a aquella que vendría a sustituir, la contenida en la anteriormente criticada Decisión Marco 2008/977/JAI.

La primera y más evidente, se deriva del hecho de que, al tener forma de Directiva y no de Decisión Marco como su predecesora, conseguirá que su articulado

[38] PEYROU, S., op. cit. ant., pp. 150 y ss.
[39] TINNEFELD, M. T./ BUCHNER, B. /PETRI, T., op. cit. ant., p. 124; PEYROU, S., op. cit. ant. p. 152, SOLAR CALVO, P., op. cit., ant., entre otros.
[40] COM (2012) 0011.
[41] COM (2012) 0010.
[42] PEYROU, S., op. cit. ant., p. 153.

tenga un efecto directo sobre las normativas nacionales, lo que sin duda incrementará su eficacia de armonizadora[43], por más que continúe permitiendo que existan ciertas divergencias entre tales ordenamientos, al otorgar a sus respectivos legisladores cierto margen de maniobra a la hora de decidir el modo en que cumplir con lo que la misma les exigiría que consiguiesen[44]; efecto que, además, y por otra parte, se verá notablemente intensificado como consecuencia de que la proyectada regulación no limite ya su ámbito de aplicación, tal y como hace la todavía vigente Decisión Marco, a los intercambios transfronterizos de datos, sino que también prevea su aplicación con respecto a los tratamientos puramente nacionales[45].

Sin embargo, y frente a todos estos importantes avances, hay que reconocer, como señala el Supervisor Europeo de Protección de Datos (SEPD) en su dictamen de 7 de marzo de 2012, referido al comentado paquete legislativo, que la Directiva propuesta también presenta notables deficiencias.

Así, por ejemplo, resulta altamente criticable que, a pesar de que sus artículos 5 y 6 obliguen a los Estados miembros a distinguir los datos personales que traten con fines penales, dependiendo de a quien estuviesen referidos (sospechosos, condenados, víctimas, testigos, etc..), de su grado de fiabilidad y exactitud o de si estaban referidos a personas o a hechos, no prevea, sin embargo, ninguna consecuencia ni efecto práctico para dicha clasificación; o que continúe dejando completamente en manos de las normativas estatales la determinación de cuestiones tan fundamentales para la protección de los derechos de los ciudadanos, como las de los plazos máximos que las autoridades competentes podrán almacenar sus datos personales, sin contar con el consentimiento o voluntad de su titular.

---

[43] SOLAR CALVO. P., op. cit. ant.

[44] TINNEFELD, M. T./ BUCHNER, B. /PETRI, T., op. cit. ant., p. 125. Esto último ha sido, sin embargo, criticado por PEYROU, S. quien pone de manifiesto el hecho de que resultaría mucho más efectivo, a la hora de reducir la fragmentación jurídica existente, haber establecido dicha normativa mediante un reglamento, como se ha hecho a la hora de regular la protección general de los datos utilizados con otros fines, en op. cit. ant., p.154.

[45] Así lo indica, por ejemplo, PEYROU, S., op. cit. ant., p. 157; TINNEFELD, M. T./ BUCHNER, B. /PETRI, T. quienes, sin embargo, destacan que quedan al margen de su ámbito de aplicación los tratamientos de datos realizados por las instituciones de la UE (que se han de ajustar a lo establecido por el Reglamento (CE) 45/2001, de 18 de diciembre de 2000 y otras normas específicas) y las actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión, como las relativas a la seguridad nacional (artículo 2.3 de la Propuesta de Directiva) op. cit. ant., p. 134; excepción ésta que, curiosamente, y como señala SOLAR CALVO, P. podría llevar a que se mantengan al margen de dicha norma europea todos los tratamientos de datos de carácter personal que se realicen con fines de prevención, investigación, prevención, detección o enjuiciamiento de delitos terroristas, en Op. cit. ant.

Tampoco parece aceptable que establezca unos requisitos y garantías realmente débiles a la hora de autorizar que dichos datos se puedan transferir a terceros países diferentes de los integrantes de la UE y que, consecuentemente, no estarían dentro del ámbito de aplicación de las garantías que prevé la propia Directiva o, lo que es incluso peor, que su artículo 59 deje vigentes e inalterados los articulados del numeroso elenco de normas especiales que regulan el complejo «patchwork» normativo actualmente existente en la UE en relación a los tratamientos de los que nos venimos ocupando, lo que, evidentemente, redundará en una significativa merma de las garantías de los derechos de los ciudadanos[46].

Otra crítica que se debe hacer a la comentada norma se deriva del hecho de que parezca contemplar la posibilidad de que el régimen excepcional que establece para los tratamientos realizados con fines penales, se pueda también llegar a utilizar para perseguir fines distintos de los exclusivamente referidos a la prevención, investigación o represión de delitos.

Así se deduce del hecho de que su artículo 7 establezca que los Estados miembros dispondrán que los tratamientos de datos personales a los que dicha norma se refiere serán lícitos, tanto si se realizan, por parte de la autoridad competente, para ejecutar las tareas tendentes a lograr los fines de los que habla su artículo 1.1., esto es para, prevenir, investigar o sancionar alguna infracción penal, como si se utilizan *«b) para cumplir con una obligación jurídica a la que esté sujeto el responsable del tratamiento*», *«c) con el fin de proteger intereses vitales del interesado u otra persona»* o *«d) a fin de prevenir una amenaza inminente y grave para la seguridad pública»*, amenaza que, evidentemente y por pura coherencia, no podrá tener carácter delictivo, ya que ello llevaría a que su expresa previsión resultase redundante y careciese de cualquier sentido.

La pregunta es inmediata, ¿podrían utilizarse entonces, conforme a lo establecido en esta nueva Directiva, unos datos que hubiesen sido recogidos, con limitaciones de los derechos de sus titulares, por ser necesarios para realizar una investigación de un delito, para realizar un posterior tratamiento que persiguiese otro fin diferente, aunque

[46] Sobre este informe GONZÁLEZ MURUA. A. R., op. cit. ant., p. 245. Respecto al mantenimiento de la fragmentariedad normativa existente en esta materia, señala PEYROU, S., que el sistema de evaluación de la aplicación del contenido en de esta Directiva, previsto en el artículo 61 de su proyectado texto y que obliga a la Comisión a evaluar su efectividad armonizadora tras tres años desde su entrada en vigor, no impedirá que dicha profusa y completa normativa siga estando vigente por un periodo que se considera inaceptable por parte del SEPD. En op. cit. ant., p.155.

legítimo, como podría ser la prevención de alguna alteración pública no delictiva o la resolución de un procedimiento administrativo sancionador?

La respuesta atendiendo a lo dispuesto en el referido precepto parece que tiene que ser afirmativa, con lo que no debe extrañar que nos asalten las dudas sobre la compatibilidad de esta nueva normativa con las exigencias derivadas del respeto al derecho fundamental a la protección de datos personales del artículo 8 CDFUE.

Habrá que afirmar, en consecuencia, como de hecho hace el propio SEPD, que el panorama normativo referido a los tratamientos de datos de los que nos venimos ocupando, continuará siendo «extremadamente decepcionante» en lo que se refiere a la garantía y tutela del derecho a la protección de datos de carácter personal, incluso si se llega finalmente a aprobar la proyectada Directiva[47]; panorama que, sin embargo y a nuestro modo de ver, habrá de cambiar de forma radical en un futuro cercano, no como consecuencia de la aprobación de ninguna norma o Tratado nuevo por parte de la UE, sino, precisamente y como en tantas ocasiones anteriores, como resultado de la emisión de una Sentencia del Tribunal de Justicia de la Unión Europea. En concreto de la que dicho Tribunal emitió el pasado 8 de abril de 2014, en relación a la Directiva de conservación de datos relativos a las comunicaciones con fines de investigación criminal, (la ya citada Directiva 2006/24/CE), resolución de la que nos pasamos a ocupar.

4.LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA DE 8 DE ABRIL DE 2014 Y SU POSIBLE REPERCUSIÓN EN LA POLÍTICA EUROPEA DE PROTECCIÓN DE DATOS PERSONALES EN MATERIA PENAL MUITO POUCO SE SABE ACERCA DO VERDADEIRO CONHECIMENTO E PODER COMPUTACIONAL E INTELECTUAL DAS AGÊNCIAS DE SEGURANÇA DAS GRANDES POTÊNCIAS MUNDIAIS, COM DESTAQUE PARA A NSA.

Muchas fueron las voces que, desde un principio, se alzaron frente al controvertido sistema de captación y almacenamiento generalizado de datos de telecomunicaciones que creó la Directiva 2006/24/CE y que obligaba a todos los

[47] Dictamen del SEPD de 7 de marzo de 2012 (2011/C 181/02).

proveedores de dicha clase de servicios a retener determinados datos externos, relativos a las comunicaciones que realizasen sus clientes, para garantizar que su realización se puedan posteriormente «trazar» o analizar, en caso de que ello fuese requerido para investigar un delito grave. Críticas que incluso se vieron judicialmente respaldadas por el hecho de que algún Tribunal Constitucional, como el alemán, llegase a declarar que parte de la ley que traspuso dicha normativa europea al ordenamiento jurídico de aquel país era incompatible con los derechos garantizados por su Carta Magna [48].

Precisamente en esta misma línea, pero más recientemente, la Corte Suprema de Irlanda y el Tribunal Constitucional de Austria plantearon sendas peticiones de Decisión prejudicial ante el Tribunal Europeo de Justicia, (asuntos C-293/12 y C-594/12 respectivamente), en las que solicitaban a dicho Tribunal que aclarase si ya el propio texto de la Directiva de conservación de datos era compatible o no con los derechos a la vida privada y a la protección de datos de carácter personal contemplados en los artículos 7 y 8 de la CDFUE, cuyo respeto, como ya vimos, resulta directamente vinculante para la propia Unión y judicialmente exigible ante dicho Tribunal, tras la entrada en vigor del Tratado de Lisboa[49].

Ambas peticiones fueron acumuladas por el Tribunal europeo y se resolvieron finalmente en su muy reciente sentencia de 8 de abril de 2014.

En esta Sentencia, el citado Tribunal afirmó que, dado que las captaciones y almacenamientos de datos que se efectúan conforme a lo establecido en la citada Directiva indudablemente limitan o interfieren en los derechos a la vida privada y a la protección de datos personales protegidos por los mencionados preceptos de la

[48] Véase a este respecto lo establecido en la Sentencia del BverG, de 2 de marzo de 2010, en la que se declara inconstitucional la normativa alemana que transponía esta Directiva por violar los principio de proporcionalidad y de determinación jurídica o claridad legal, comentada, entre otros, por ORTIZ PRADILLO, J. C. «Tecnología *versus* Proporcionalidad en la investigación Penal: La nulidad de la ley Alemana de conservación de datos de tráfico de las comunicaciones electrónicas», en *La Ley Penal* núm. 75, 2010, en <www.laley.es> (últ. vis. 2-5-2012). No faltaron tampoco las voces en España que desde un primero momento pusieron en tela de juicio la legitimidad del sistema establecido por esta Directiva por considerarlo incompatible con el principio de proporcionalidad. Véase a este respecto, por ejemplo, lo comentado por GONZÁLEZ LÓPEZ. J. J. «La retención de datos de tráfico de las comunicaciones en la Unión europea: Una aproximación Crítica», en *La LEY* núm. 6456, 2006, en <www.laley.es> (últ. vis. 10-5-2012), entre otros.

[49] En concreto, la Corte Suprema Irlandesa presentó su petición el 11 de junio de 2012, como consecuencia de la demanda presentada la Sociedad Digital Rights, dedicada a la promoción y protección de los derechos civiles y ciudadanos contra la normativa de aquel país que transpuso dicha directiva; mientras que Tribunal Constitucional de Austria presentó la suya el 19 de diciembre del mismo año, como consecuencia de los recursos interpuestos contra la normativa de aquel país por el Estado de Kärntner, el Sr. Seitlinger y otros 11.130 demandantes más.

CDFUE, se hacía necesario analizar si tal interferencia o limitación podía quedar, sin embargo, justificada atendiendo a lo establecido en el artículo 52 la propia Carta, donde se afirma que *«… cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades»*, para afirmar a continuación que *«… sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás»*.

Partiendo de esta base, el Tribunal europeo señaló que, si bien era cierto que la cuestionada Directiva afectaba a los citados derechos fundamentales, no llegaba, sin embargo, a lesionar sus respectivos contenidos esenciales, ya que, ni lesionaba el contenido esencial del derecho a la vida privada, al no ser una norma que permitiese conocer el contenido de lo que los ciudadanos comunicasen a través los medios a los que sus prescripciones les eran aplicables, ni afectaba al núcleo del derecho fundamental a la protección de los datos personales, ya que establecía ciertas medidas de protección de los datos captados frente a posibles abusos o actuaciones accidentales precisamente para salvaguardar lo fundamental de dicho derecho.

Tampoco consideró el Alto Tribunal que se pudiese cuestionar que la finalidad perseguida por la Directiva analizada, la de asegurar que los datos estuviesen disponibles a efectos de investigación, detección y persecución de delitos graves, no fuese un fin u objetivo perfectamente legítimo y de interés general, cuya búsqueda podría contraponerse a los citados derechos fundamentales, llegando incluso a legitimar su limitación. De hecho, así parecería indicarlo el hecho de que el propio artículo 6 de la CDFUE reconozca que todas las personas tienen derecho tanto a la libertad, como a la seguridad, contraponiendo, de esa forma, al primer valor, la libertad y sus garantías, con aquel otro que el comentado sistema de captación de datos trataría de alcanzar, el de la seguridad[50].

Es por ello, por lo que el Tribunal europeo entendió que la cuestión fundamental a dilucidar en los asuntos que ante él se habían planteado, sería la relativa a si las concretas limitaciones de derechos establecidas por el sistema contenido en la

[50] En concreto, el artículo 6 CDFUE establece que *«Toda persona tiene derecho a la libertad y a la seguridad»*.

cuestionada Directiva respondían o no a las exigencias derivadas del principio de proporcionalidad en sentido estricto; cuestión que obligaba a analizar, en primer lugar, si su imposición resultaría adecuada o no para conseguir la finalidad supuestamente justificaba su existencia, para después estudiar, si las concretas restricciones de derechos que iba a imponer para alcanzarla habrían quedado realmente limitadas a aquellas que resultaban estrictamente necesario imponer para hacerlo.

La primera de las cuestiones fue rápidamente resuelta por el Tribunal, ya que entendió como innegable que la captación de los datos relativos a las comunicaciones resultaba perfectamente adecuada e idónea para facilitar la investigación y persecución de delitos, sobretodo, teniendo en cuenta el papel fundamental que dichas comunicaciones han adquirido en la sociedad de la información en la que vivimos

Mucho más cuestionable resultaba, sin embargo, la segunda. Esto es, que se pueda realmente afirmar que el uso previsto para esta herramienta limitadora de derechos fundamentales hubiese quedado verdaderamente limitado a aquel que resultaba estrictamente necesario efectuar para perseguir tan legítimo fin.

En concreto, el TEJ consideró que la comentada Directiva vulneraría dicho límite con respecto al derecho a la protección de datos establecido en el artículo 8 CDFU, al permitir, por ejemplo, que el nivel de las medidas de seguridad que los proveedores tendrían que imponer, para evitar posibles abusos con respecto a dichos datos, pudiese depender de una valoración de los costes que su implantación podría llegar a generarles a dichos sujetos y también al autorizar que los datos que los mismos captasen y almacenasen pudiesen ser transferidos a terceros países, ajenos a la UE, donde su uso o posible abuso escaparía por completo al control de las autoridades independientes que, conforme a lo establecido en el apartado 3 del citado artículo de la CDFUE, deben garantizar el respeto a dicho derecho.

Tampoco respondía a las exigencias derivadas del principio de proporcionalidad el hecho de que la comentada Directiva implante un sistema de captación y almacenamiento general de los datos externos referidos a todas las comunicaciones, que lleve a que tales datos se puedan e incluso se tengan que recopilar y almacenar, aun cuando no exista indicio alguno, ni siquiera remoto, de que estuviesen relacionados con la comisión de un delito grave, o cuando se sepa incluso que estaban

referidos a comunicaciones efectuadas por personas que estaban amparadas y obligadas a mantener el secreto profesional. Esto resulta, a juicio del Alto Tribunal, absolutamente desmedido y, por tanto, desproporcionado, como también lo será que la citada norma comunitaria ordene que los datos captados se almacenen por un periodo mínimo de 6 meses, olvidando así que no todos los datos captados son igualmente útiles para perseguir e investigar delitos, con lo que la prolongación del almacenamiento de algunos de ellos carecerá de sentido a tales efectos y resultará, por tanto, también manifiestamente innecesaria y desproporcionada.

Pero es que además, tampoco resulta posible mantener que las restricciones de derechos establecidas por esta Directiva hayan quedado realmente limitadas a las que resulta estrictamente necesario imponer para perseguir delitos graves, cuando su articulado ni determina que comportamientos deben considerarse como tales[51], ni establece ninguna limitación o control que garantice que sus restricciones no se puedan emplear para perseguir otro tipo de conductas diferentes de las finalmente se lleguen a tener como verdaderos delitos graves[52].

---

[51] De hecho, sobre la interpretación y delimitación de este concepto, del de delito grave, existe todavía una viva polémica doctrinal y jurisprudencial, ya que mientras algunos autores y tribunales parten de el mismo debe ser interpretado conforme a la clasificación de los delitos que realiza nuestro Código penal en su artículo 33 CP; otros, como, por ejemplo, RODRÍGUEZ LAINZ, J. L. en «Hacia un nuevo entendimiento de gravedad del delito en la Ley de conservación de Datos relativos a las Comunicaciones Electrónicas», *LA LEY* núm. 7789, 2012 <www.laley.es> (últ. vis. 4-2-2014) o en «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», cit. ant., propugnan una interpretación mucho más flexible y que no atienda tan solo a la concreta pena con la que el legislador sancione las conductas en cuestión, sino también otros factores, como la «relevancia social del hecho» o su repercusión; conceptos todos ellos altamente indeterminados y difusos, cuya concreción puede depender de criterios puramente subjetivos o incluso de factores tales como la importancia que los medios de comunicación decidan darle al hecho en cuestión, lo que nos lleva a rechazar su posible aplicación en este contexto, tal y como hace, por ejemplo, CORTÉS BECHIARELLI, E. por entender, como este autor, que el uso de tales conceptos no solo puede llevar a que los jueces se arroguen funciones casi legislativas en esta materia, sino también a que se olvide que cuando el legislador impone una pena de forma abstracta para un delito, es porque ha valorado y determinado la gravedad de su realización en la propia ley que lo castiga. En *El delito de corrupción deportiva.* Ed. Tirant lo Blanch, Valencia 2012 .p. 217.

[52] Ha de señalarse en este sentido, que aún a día de hoy, continúa habiendo una viva polémica doctrinal y jurisprudencial en nuestro país sobre las condiciones y requisitos procesales que han de cumplirse para poder acceder a dichos datos, ya que mientras algunas sentencias, como la STS 236/2008, de 9 de mayo, mantienen que dichos datos están disponibles para cualquiera de las autoridades responsables de la persecución e investigación de delitos de las que habla la Ley 25/2007, de 18 de octubre de 2007, de conservación de datos de comunicaciones electrónicas y redes públicas de comunicación, algunos autores, entre los que me incluyo, consideramos que el artículo 7 de dicha ley obliga expresamente a contar con una autorización judicial para acceder a los mismos, ya que su acceso afecta también al derecho fundamental al secreto de las comunicaciones, tal y como ha afirmado el TEDH en reiterada jurisprudencia, desde su célebre Sentencia de 2 agosto 1984, referida al denominado «caso *Malone vs Reino Unido*». Sobre esta polémica véase lo comentando, por ejemplo, por FRIGOLS I BRINES, E. «La protección constitucional de los datos de comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a intimidad a la luz del uso de las nuevas

Todo ello llevó al TEJ a considerar que la comentada Directiva resultaba completamente incompatible con lo establecido en el CDFUE, por lo que debía considerarse inválida y carente de todo efecto. Pero también y paralelamente, le llevó a establecer una serie de criterios o referentes que habrán de ser tenidos muy en cuenta a la hora de valorar la posible compatibilidad con las prescripciones contenidas en dicha Carta protectora de los derechos fundamentales, de cualquier normativa que se haya creado o se vaya a crear con el fin de regular los sistemas de tratamientos de datos personales a los que hemos dedicado este trabajo.

Veamos por ello, a continuación y aunque sea someramente, en qué medida dichos referentes o pronunciamientos judiciales deberían influir tanto en la normativa europea actualmente vigente en relación a dichos tratamientos, como sobre los proyectos que la UE vienen tramitando, precisamente y según se nos dice, con el fin de crear un nuevo y más garantista marco regulador para los mismos.

5.LA UNIÓN EUROPEA ANTE LA ENCRUCIJADA. ¿HACIA UNA NUEVA POLÍTICA CRIMINAL REFERIDA A LOS TRATAMIENTOS DESTINADOS A LA PREVENCIÓN, INVESTIGACIÓN Y PERSECUCIÓN DE DELITOS?

Lo comentado hasta el momento ha puesto de manifiesto que la regulación europea referida a los tratamientos de datos con fines de prevención o represión criminal ha vivido hasta el momento dos fases claramente diferenciadas.

Una inicial, caracterizada primordialmente por la creación de instrumentos tendentes a facilitar y favorecer la cooperación y el intercambio de datos e informaciones entre las diferentes administraciones nacionales y supranacionales competentes en materia penal y que culminó con el desarrollo del principio de disponibilidad, y otra, más cercana en el tiempo, en la que la garantía del respeto a los derechos fundamentales de los ciudadanos y entre ellos, destacadamente, los de intimidad y protección de datos de carácter personal, ha comenzando paulatinamente a reclamar el papel que le corresponde y deberían haber tenido, desde un primer momento, en dicha regulación.

---

tecnologías», en *La protección jurídica de la Intimidad*. Ed. Iustel. Madrid, 2010, pp. 45 y ss. o por mí mismo, en GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas?..»., cit. ant., p. 46.

Esta segunda fase ha tenido, sin duda, en la aprobación del Tratado de Lisboa un hito fundamental, pero, por el momento y pese a lo declarado, tanto en dicho Tratado como en el Programa de Estocolmo o en la Agenda Digital para Europa, solo ha dado lugar a la elaboración de un proyecto de Directiva que resulta, como hemos visto, «extremadamente decepcionante» en términos de garantías.

Es precisamente, en este momento, cuando la emisión de la anteriormente comentada Sentencia del Tribunal Europeo de Justicia ha venido a aportar un pequeño rayo de esperanza en tan oscuro y decepcionante panorama normativo, ya que no solo ha dejado completamente claro que las limitaciones de los derechos a la intimidad o a la protección de datos de las personas que se creen para prevenir, investigar o reprimir delitos graves, solo resultarán legítimas en la medida en que se establezcan para perseguir tal fin y no otro, y queden limitadas a las que resulten estrictamente necesarias para conseguirlo, sino que, además y al mismo tiempo, también ha señalado que tendrá que ser el regulador europeo que implante tales restricciones, y no el nacional, quien habrá de definir y establecer los criterios o elementos objetivos que tendrán que garantizar que las mismas no sobrepasen las barreras de lo que es estrictamente necesario hacer para alcanzar dicha finalidad.

Los efectos que estas declaraciones judiciales han de tener sobre la materia que nos ocupa son, a nuestro modo de ver, extremadamente relevantes.

Así, por ejemplo resulta evidente que, una vez que el Tribunal Europeo de Justicia ha señalado, de forma tajante, que será precisamente la persecución de los fines penales señalados y no la de otros posibles objetivos o motivos[53], la que podrá

[53] En este sentido resulta interesante destacar que algunos autores, como TINNEFELD, M. T./ BUCHNER, B. /PETRI, T. señalan que lo que impide que el proyecto de Directiva para la protección de datos personales en los tratamientos con fines de prevención y represión penal de la que venimos hablando, contemple al consentimiento como posible causa de autorización del tratamiento de dichos datos, será que la existencia relación de subordinación existente entre el titular de los datos y la administración que se encarga de esta materia, hará inviable que dicho el consentimiento emitido por el ciudadano pueda tener efectos jurídicos, atendiendo a lo que vendrá a establecer el nuevo Reglamento General de Protección de datos que se tramita de forma paralela a dicha Directiva, por no haberse emitido en una situación de verdadero equilibrio, en op. cit. ant., p. 135. No creemos, sin embargo, que ello sea del todo correcto, ya que dicha afirmación se sustenta en la existencia de una relación de sometimiento o subordinación del ciudadano ante la administración que no se ajusta a los parámetros conforme a los que esta última deba actuar en un verdadero Estado democrático y de Derecho. En realidad, en los Estados realmente democráticos el ciudadano no está para servir a la administración, sino la administración para servir al ciudadano, siendo precisamente dicho hecho el que impide que la administración pueda los derechos de las personas, salvo que ello resulte estrictamente necesario para perseguir un fin legítimo y de interés general. En concreto, y en el caso que nos ocupa las restricciones de derechos establecidas en la Directiva se sustentarían en la necesidad de posibilitar las investigaciones de delitos, siendo dicho hecho y no la relación de subordinación existente entre

legitimar el régimen excepcional y las restricciones de derechos que se permiten en los tratamientos de datos personales de los que nos venimos ocupando, se obliga al regulador europeo a revisar tanto la normativa vigente, como la que pretenda crear en el futuro en relación a los mismos, para garantizar que dichas normativas excluyan cualquier posibilidad de que su absolutamente excepcional regulación pueda ser utilizada para efectuar tratamientos con fines distintos de los estrictamente penales, ya que ello evidentemente llevaría a que tales tratamientos alternativos se efectuasen empleando algunas restricciones de derechos fundamentales que, si bien podrían resultar necesarias y proporcionadas en relación a la persecución de finalidades penales, no tendrían por qué serlo con respecto a estos nuevos y alternativos objetivos.

Habrá pues, que revisar, incluso antes de su aprobación, tanto el proyecto de Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves[54], como la ya citada propuesta Directiva de protección de datos personales en los tratamientos realizados con fines penales, que en estos momentos se tramitan en el seno de la UE, con el fin de garantizar que sus articulados excluyan cualquier posibilidad de que sus excepcionales prescripciones puedan utilizarse para perseguir fines diversos a los puramente penales; pero también, y por otra parte, habrá que comprobar en profundidad la numerosa normativa europea vigente relativa a los tratamientos de datos personales con finalidades penales y que, no lo olvidemos, se pretende dejar inalterada tras la aprobación de dichas Directivas, para evitar que ninguna de sus prescripciones pueda permitir, por ejemplo, que las autoridades receptoras de los datos personales enviados desde otro Estado miembro, para facilitar

---

ciudadano y Estado, la que permitirá que la administración pueda obtener y procesar los datos del primero sin contar con su consentimiento, lo que evidentemente en modo alguno supondrá, frente a lo que sostienen TINNEFELD, M. T./ BUCHNER, B. /PETRI, T. que las administraciones no puedan e incluso tengan que contar con dicho consentimiento para tratar los datos de los ciudadanos para fines diferentes de los puramente penales.

[54] Esta propuesta de Directiva [COM (2011) 32 final], de 2 de febrero de 2011, conocida como por la propuesta de Directiva PNR, como consecuencia del acrónimo de la denominación inglesa *Passanger Name records*, y que trata de armonizar las diferentes normativas estatales referidas a los tratamientos de los datos de los pasajeros para luchar contra el terrorismo, ha recibido múltiples críticas tanto doctrinales, como del propio Grupo del artículo 29 o el SEPD, lo que, como señala KAINER, F., ha llevado a que su posible aprobación haya sido parada, por lo menos por el momento, por el Parlamento europeo, en «Strafrecht im Raum der Freiheit, der Sicherheit und des Rechts. Entwicklung und Umsetzungsprobleme des europäisierten Strafrechts in Deutschland» en Eur-Bei, 87, 2013, p. 108. Sobre los problemas de todo tipo que este texto normativo presenta, véase lo comentado, por ejemplo, por PEYROU, S., op. cit. ant., pp. 160 y ss.

una investigación penal, puedan utilizarlos para fines diferentes de los puramente penales, simplemente porque las autoridades del Estado emisor se lo hubiese autorizado[55].

Lo lógico, a nuestro modo de ver, para acabar con todo este despropósito normativo y para dar, al mismo tiempo, cumplimiento a lo exigido por el Tribunal Europeo de Justicia, será convertir a la nueva Directiva de protección de datos personales en esta clase de tratamientos en una norma general, de aplicación a todos los sistemas destinados a cumplir con fines de prevención o prevención de delitos, que garantice, entre otras cosas, que ninguno de ellos se puedan utilizar para fines diferentes de aquellos que legitimaron su creación, esto es, tal y como expresamente afirma el artículo 1 de la propuesta de Directiva que venimos comentando, para la *«… prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales»*.

Para ello, se debería modificar lo establecido en los artículos 7 y 59 de dicha propuesta. Pero también y por otra parte, sería conveniente que se regulase, de forma específica, mediante la creación de normas especiales, adecuadas y completamente autónomas de las referidas a los propiamente penales, los tratamientos de datos realizados con fines no penales que pudiesen necesitar del establecimiento de determinadas excepciones al régimen general de protección de este tipo de datos, para poder cumplir con la finalidad para la que se realizasen (p. ej. los destinados a la persecución y sanción de infracciones administrativas, a la recaudación de impuestos o aranceles o a la salvaguarda de algún derecho de los ciudadanos).

---

[55] La trascendencia de esta cuestión ha quedado, de hecho, reflejada en algunos casos concretos que ya se han planteado, como el que se presentó cuando el Comité Olímpico Nacional Italiano solicitó que al Juzgado de instrucción núm. 31 de Madrid le hiciese llegar las muestras de sangre que había recogido en uno de los registros domiciliarios que se realizaron en el marco de la denominada «Operación Puerto», o cuando poco después fue la propia Federación española de ciclismo la que solicitó su entrega a efectos de tramitar los correspondientes expedientes administrativos sancionadores contra los sujetos que se vieron envueltos en este conocido caso de dopaje, sin llegar, sin embargo, a tener responsabilidad penal por ello (los propios deportistas que utilizarían las sustancias ilegales). Pese a lo contradictorias que han resultado hasta el momento las resoluciones emitidas por nuestros tribunales con respecto a este tipo de casos, creemos que hay que entender, como de hecho hacen COLOMER HERNÁNDEZ, I. en «La transmisión y cesión de datos personales obtenidos en un proceso penal a un procedimiento sancionador por dopaje», en *RDDE* 2013, pp. 32 y ss. o CORTÉS BECHIARELLI, E., op. cit. ant., pp. 219 y ss., que los indicios o pruebas que se obtienen vulnerando legítimamente derechos fundamentales, como la inviolabilidad domiciliaria, el secreto de las comunicaciones o el propio derecho de protección de datos de carácter personal, por haberse recopilado para realizar una investigación criminal, nunca deberían poder usarse para investigar y, en su caso, sancionar unos hechos que no tuviesen dicha condición, esto es, para investigar y sancionar, por ejemplo, una mera infracción administrativa, por muy grave que ésta fuera.

Todo ello, plantea, sin duda, un reto reformador enorme para el regulador europeo; reto que, además, se verá incrementado como consecuencia de que dicho regulador también estará obligado, atendiendo a lo establecido en la comentada Sentencia del TEJ, a revisar por completo tanto el proyecto de Directiva del que venimos hablando, como el resto de normas reguladoras de los diferentes sistemas de tratamiento de datos con fines penales que ha creado y pretenda crear en el futuro, para garantizar que sean sus articulados, y no los de las normativas nacionales que los traspongan, los que realmente definan los plazos, límites y condiciones que habrán de garantizar que las restricciones del derecho fundamental a la protección de datos personales que impongan nunca y bajo ninguna circunstancia puedan ir más allá de las que resultaría estrictamente necesario aplicar, para que tales sistemas puedan cumplir con la finalidad para la que se crearon, la de prevenir, investigar, perseguir y sancionar los delitos graves que se puedan llegar a cometer[56].

[56] Entendemos en tal sentido, que lo establecido por la comentada Sentencia del TEJ obligará, entre otras cosas, a replantearse si todas las restricciones de derechos que define y limita la citada propuesta de Directiva, pueden aplicarse con independencia de la gravedad de la infracción penal con respecto a la que se aplique, o debe definirse un mínimo de gravedad, posiblemente atendiendo a la posible pena abstracta prevista para la infracción en cuestión, que garantice que tales limitaciones solo se puedan aplicar con respecto a la persecución o represión de infracciones que resulten realmente graves. Por otra parte, la comentada Sentencia también obligará a revisar el sistema de transmisión a terceros países establecido por los artículos 33 y siguientes de la propuesta y a que haya de replantearse lo establecido en sus artículos 15 y 16, con respecto a las restricciones de los derechos de rectificación y supresión de datos personales de los ciudadanos, ya que tales preceptos deberían fijar de forma clara los criterios objetivos que servirían para garantizar que dichos derechos solo se vean limitados en los casos y en la medida en que resulte estrictamente necesario hacerlo, para alcanzar los fines de investigación y represión penal perseguidos por su tratamiento, no pudiendo quedar la fijación de tales criterios, tal y como pretende el actual proyecto, por lo menos en relación a la segunda de las cuestiones planteadas, exclusivamente en manos de la decisión de los reguladores estatales. En la misma línea, el comentado texto normativo tampoco podrá dejar completamente en manos de la regulación de los países miembros la determinación del distinto régimen que se habrá de otorgar a cada una las categorías de datos que los artículos 5 y 6 de la propuesta diferencian en atención a su exactitud, fiabilidad y el carácter del sujeto al que estén referidos (sospechoso, condenados, víctimas, testigos, etc.), sino que habrá de fijar su correspondiente régimen jurídico y las posibles limitaciones a los derechos que el mismo pueda suponer con respecto a los derechos de tus titulares (p. ej. innecesariedad del consentimiento del titular para su recolección, restricción al derecho a la información, denegación del derecho de cancelación, etc.), atendiendo a la especifica utilidad y relevancia que cada una de dichas clases de datos tendría, según su características y procedencia, en la prevención y persecución de delitos. En este sentido, el regulador europeo debería, a nuestro modo de ver, tener muy presente lo establecido por la Sentencia de 4 diciembre de 2008 del Tribunal Europeo de Derechos Humanos, referida al caso S. y *Marper vs Reino Unido*. En esta Sentencia, el referido Tribunal afirmó que el almacenamiento de las huellas dactilares, de muestras celulares y del perfil genético con fines de investigación criminal de personas que, como los demandantes en dicho procedimiento, ya habían sido absueltos respecto a los casos penales que motivaron la recolección de las pruebas suponía un desproporcionado e innecesario sacrificio de sus derechos fundamentales a la intimidad y a la protección de datos de carácter personal, por dar lugar a que el almacenamiento de dichos datos pudiese tener una duración que excedería de lo estrictamente necesario para conseguir las finalidades para los que los datos se habían registrado. Este hecho debería ser tenido muy en cuenta por el regulador europeo a la hora de establecer en la comentada Directiva el concreto tratamiento de los

Será, sin duda, un reto reformador formidable, pero también, y a nuestro modo de ver, uno que el regulador europeo habrá necesariamente de afrontar si realmente pretende crear un «sistema de justicia penal europeo integrado».

Para hacerlo, tal y como en su día señaló VOGEL, resulta imprescindible que todos los Estados integrados en tal sistema puedan colaborar entre sí sobre la base de la confianza y el reconocimiento mutuos, lo que exigirá que todos ellos deban poder estar seguros en que el resto respetarán los derechos humanos de todas las personas, con independencia de su nacionalidad[57]. Esta exigencia convierte, sin duda, al respeto a dichos derechos, y entre ellos, el referido a la protección de datos, no en un obstáculo o una rémora para la posible creación e implantación de una política criminal europea capaz de luchar contra las modernas formas de criminalidad inter- o transnacional, como la delincuencia informática, la económica, la medioambiental o incluso, el temible terrorismo[58], sino, precisamente, en uno de los elementos configuradores básicos de la «cultura penal común» a todos los países de la UE, que se requiere para que todos ellos, pese a las evidentes y profundas diferencias que existen entre sus respectivas tradiciones y sistemas jurídicos, puedan llegar a implantar y seguir la política criminal europea que se necesita para poder luchar coordinada y eficazmente contra tales fenómenos criminales[59].

---

datos personales deberían recibir, atendiendo a su concreta procedencia, del mismo modo que debería hacerlo la todavía vigente normativa española en la materia, la LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir de ADN, que tendría que evitar que los datos de los sospechosos no imputados se puedan retener, como permite hacerlo su artículo 9, hasta que transcurra el periodo de prescripción del delito para cuya investigación se recabaron. Esto último resulta del todo inadmisible, como señalan, por ejemplo, HOYOS SANCHO, M., «Profundización en la cooperación transfronteriza en la Unión Europea:…», cit. ant., p. 179 o por CARUSO FONTÁN, V., «Bases de datos policiales sobre identificadores obtenidos a partir del ADN y derecho a la intimidad genética», en *Foro*, vol. 15, núm. 1 (2012), pp. 163 y ss., quienes, precisamente por ello, consideran que todos estos datos deberían ser eliminados en el mismo momento en que se constate que no se han reunido elementos suficientes para proceder al enjuiciamiento del hecho cuya investigación motivó su captación. No son, por tanto, pocas las cuestiones que el regulador comunitario debe replantearse y resolver tanto a la hora de revisar tanto esta Directiva, como el resto de normas reguladoras de los procesamientos de datos personales con fines penales, lo que, sin duda, incrementa aún más la magnitud del reto reformador que el TEJ le ha exigido que comience a afrontar.

[57] VOGEL, J., «Cooperación penal: cinco tendencias. Cinco propuestas para una acción futura», cit. ant., pp. 158 y ss.

[58] No le falta, por tanto, razón a AIXALA, A. cuando afirma que existe *«… un verdadero European way of fighting terrorism, distinto y mucho más eficaz y eficiente que el estadounidense»*, caracterizado por *«combatir el terrorismo con la ley en la mano y en el marco del Estado de Derecho*. Op. cit. ant., 55, lo que, sin embargo, no nos puede hacer olvidar que también en seno de la Unión se han producido tensiones securitarias ante el fenómeno terrorista que deben ser corregidas lo antes posible, para garantizar el más absoluto respeto a los derechos fundamentales.

[59] QUINTERO OLIVARES, G. / GONZÁLEZ CUSSAC, J. L., «Sobre una política criminal común europea», en *La adecuación del Derecho penal Español al ordenamiento de la Unión europea. La política criminal europea.* Ed. Tirant lo Blanch, Valencia, 2009, pp. 39 y ss.

El reto para la política criminal europea, por tanto, está ya planteado. El camino para afrontarlo, por lo menos, en lo que se refiere a los tratamientos de datos personales realizados con fines de prevención, investigación y sanción de delitos graves, lo ha trazado el Tribunal Europeo de Justicia. Solo resta entonces que regulador europeo lo entienda y comience, de una vez por todas, a asumir la función que está llamado a desempeñar en ese Espacio Único, no solo de Seguridad, sino también de Libertad y Justicia, que la Unión Europea pretende llegar a ser.

6.BIBLIOGRAFÍA

ACED FÉLEZ, E., «Principio de disponibilidad y protección de datos en el ámbito policial» en <http://noticias.juridicas.com> (últ. vis. 11-3-2014).

APARICIO SALOM, J., *Estudio sobre la protección de datos*. Ed. Aranzadi, Cizur Menor, 2013.

AIXALA, A., «La estrategia de la UE ante el terrorismo internacional y la defensa de los derechos y libertades», p. 51, en <http://www.iuee.eu/pdf-publicacio/1/jpjdqoe8lrscpmve8of8.pdf> (últ. vis. 16-4-2014).

BLANCO QUINTANA, M. J., «La comunicación de antecedentes penales entre los Estados. El Sistema europeo de información de antecedentes penales», en *BMJ*, 2013.

CARUSO FONTÁN, V., «Bases de datos policiales sobre identificadores obtenidos a partir del ADN y derecho a la intimidad genética», en *Foro*, vol. 15, núm. 1 (2012).

COLOMER HERNÁNDEZ, I., «La transmisión y cesión de datos personales obtenidos en un proceso penal a un procedimiento sancionador por dopaje», en *RDDE* 2013.

CORTÉS BECHIARELLI, E., *El delito de corrupción deportiva.* Ed. Tirant lo Blanch, Valencia 2012.

FERNÁNDEZ OGALLAR, B., *El Derecho penal armonizado de la Unión europea.* Ed. Dykinson. Madrid, 2014.

FRIGOLS I BRINES, E., «La protección constitucional de los datos de comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a intimidad a la luz del uso de las nuevas tecnologías», en *La protección jurídica de la Intimidad*. Ed. Iustel. Madrid, 2010.

GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación», en *Revista General de Derecho penal*, núm. 19, 2013, pp. 4 y ss., en <http://www.iustel.com/> (últ. vis. 20-4-2014).

GÓMEZ-JARA DÍEZ, C., «Constitución europea y Derecho penal: ¿Hacia un Derecho penal Federal europeo?», en *Derecho penal y política transnacional*, Ed. Alitier, Barcelona, 2005.

GONZÁLEZ LÓPEZ. J. J., «La retención de datos de tráfico de las comunicaciones en la Unión europea: Una aproximación Crítica», en *La LEY* núm. 6456, 2006, en <www.laley.es> (últ. vis. 10-5-2012).

GONZÁLEZ MURUA, A. R., «El supervisor Europeo de protección de datos ante la revisión del marco jurídico de la protección de datos. Especial referencia a las reformas en el seno del espacio de libertad, seguridad y justicia», en *El espacio de libertad, seguridad y justicia: Schengen y Protección de datos*. Ed. Aranzadi, Cizur Menor, 2013.

GUICHOT, E., *Datos personales y administración pública,* Ed. Aranzadi, Cizur Menor (Navarra) 2005.

HOYOS SANCHO, M., «Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos», en *Espacio europeo de libertad, seguridad y justicia: Últimos avances en cooperación judicial penal*. Ed. Lex Nova. Valladolid, 2010.

KAINER, F., «Strafrecht im Raum der Freiheit, der Sicherheit und des Rechts. Entwicklung und Umsetzungsprobleme des europäisierten Strafrechts in Deutschland» en *Eur-Bei*, 87, 2013.

MAPELLI MARCHENA, C., *El modelo penal de la Unión europea*. Ed. Aranzadi, Cizur Menor, 2014.

NIETO MARTÍN, A., «Posibilidades y límites de la armonización del Derecho penal nacional tras Comisión v. Consejo. (Comentario a la STJCE, asunto C-176/03, de 13-9-2005)». *REDE* núm. 17, 2006.

OERMANN, M., *Individualdatenschutz im europäischen Danteschutzrecht*. V Centauros, Freiburg. 2012.

ORTIZ PRADILLO, J. C., «Tecnología *versus* Proporcionalidad en la investigación Penal: La nulidad de la ley Alemana de conservación de datos de tráfico de las comunicaciones electrónicas», en *La Ley Penal* núm. 75, 2010, en <www.laley.es> (últ. vis. 2-5-2012).

PARIENTE DE PRADA, I., *El Espacio de libertad, Seguridad y justicia: Schengen y protección de datos.* Ed. Azanzadi. Cizur Menor, 2013.

PEYROU, S., «Algunas reflexiones sobre la protección de datos en el ELSA o la crónica de una esperanza frustrada», en *El espacio de libertad, seguridad y justicia: Schengen y Protección de datos*. Ed. Aranzadi, Cizur Menor, 2013.

QUINTERO OLIVARES, G. / GONZÁLEZ CUSSAC, J. L., «Sobre una política criminal común europea», en *La adecuación del Derecho penal Español al ordenamiento de la Unión europea. La política criminal europea.* Ed. Tirant lo Blanch, Valencia, 2009.

RECUERO, P., «La protección de datos y Schengen: Una visión desde la experiencia española», en *El Espacio de libertad, seguridad y justifica: Schengen y protección de Datos*. Ed. Aranzadi. Cizur Menor, 2013.

RODRÍGUEZ LAINZ, J. L., «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», en *LA LEY* núm. 6859 y 6860, 2008, en <www.laley.es> (últ. vis. 12-2-2014).

- «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: Derecho derivado», en *LA LEY* núm. 7373, 2010 en <www.laley.es> (últ. vis. 12-4-2014).

- «Hacia un nuevo entendimiento de gravedad del delito en la Ley de conservación de Datos relativos a las Comunicaciones Electrónicas», *LA LEY* núm. 7789, 2012 <www.laley.es> (últ. vis. 4-2-2014).

SCHÜNEMANN, B., «Forschritte und Fehltritte in der Strafrechtspflege der EU», en GA, 2004.

SANTOS GARCÍA, D., *Nociones generales de la Ley orgánica de protección de datos y su reglamento: adaptado al RD 1.720/2007 de 21 de diciembre*. Ed. Tecnos, 2012.

SILVA SÁNCHEZ, J. M., «Los principios inspiradores de las propuestas de un Derecho penal europeo. Una aproximación Crítica», *RP* núm. 13, 2004.

SOLAR CLAVO, P., «La doble vía europea en protección de datos», en LA LEY núm. 2832, 2012, en <www.laley.es> (últ. vis. 10-4-2014).

TIEDEMANN, K., «EG und EU als Rechtquellen des Strafrechts» en *Festschrift für Claus Roxin.* V Walter Gruyter. Berlín. Nueva York, 2001.

TINNEFELD, M. T./ BUCHNER, B. /PETRI, T., *Einführung in das Datenschutzsrecht.* V. Oldenburg, München, 2012.

VOGEL, J., «Política criminal y dogmática penal europea», en *RP* núm. 11, 2003.

-«Cooperación penal: cinco tendencias. Cinco propuestas para una acción futura», en *El Derecho penal de la Unión europea. Situación actual y perspectivas de futuro.* Ed. UCLM. Cuenca, 2007.

-«EU-Arbeitsweisevertrag Artículo 82 Gegenseitige Anerkennung; Angleichung», en *Das Recht der Europäischen Union.* 51 Ergänzungslieferung, V. Becks, München, 2013.