REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.
ISSN 2530-4496 – AÑO 1, N° 6, 2019, PÁGS. 49-74

NUEVOS HORIZONTES PARA EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES, AL AMPARO DEL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y DE LA DIRECTIVA RELATIVA AL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO PENAL.

NEW HORIZONS FOR THE RIGHT RIGHT OF PROTECTION OF PERSONAL DATA. THE PROCESSING OF PERSONAL DATA, BASED ON NEW GENERAL DATA PROTECTION REGULATION AND THE DIRECTIVE RELATING TO THE PROCESSING OF PERSONAL DATA IN THE CRIMINAL FIELD.

María Elena Laro González[1]

1 Licenciada en Derecho por la Universidad de Sevilla. Máster Superior en Abogacía por la Universidad Pablo de Olavide.

RESUMEN[1]

Las nuevas tecnologías hacen necesario que se refuercen los derechos de los interesados, en aras a preservar el derecho fundamental a la protección de datos personales. En este contexto, la Unión Europea ha promulgado el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta a sus datos personales y la libre circulación de esos datos. En el ámbito de la cooperación judicial penal, se ha promulgado la Directiva (UE) 2016/680, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

PALABRAS CLAVE

Derecho de protección de datos; tecnología; intercambio de datos; Unión Europea; cooperación judicial penal.

ABSTRACT

The new technologies make it necessary to strengthen the rights of the interested, to preserve the fundamental right to the protection of personal data. In this context, the European Union has promulgated Regulation (UE) 2016/679, from 27 April of 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. In the context of criminal judicial cooperation, has promulgated the Directive (UE) 2016/680, from 27 April of 2016, relative on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

KEYWORDS

Right of protection of personal data; technology; data exchange; European Union; judicial criminal cooperation;

INTRODUCCIÓN

En el actual contexto criminal resulta evidente que las nuevas formas de delincuencia organizada han propiciado nuevos paradigmas en la prevención y persecución de delitos. La libre circulación de personas[2], en el territorio de la Unión Europea (en adelante, UE), ha contribuido a que los delincuentes no tengan fronteras para la perpetración de delitos, buscando, éstos, los refugios legislativos que le lleven a conseguir la impunidad. En este orden de cosas, se hace necesario reforzar la cooperación policial y judicial penal, donde la orientación vaya encaminada hacia la seguridad de los Estados miembros como forma combativa de la delincuencia organizada.

1. Esta contribución ha sido realizada en el marco de una estancia de investigación en el Instituto de Estudios Europeos de la Universidad de Valladolid, en el curso académico 2018-2019. El presente trabajo ha sido realizado en el marco del proyecto I+D+I *"Instrumentos de reconocimiento mutuo y ejecución de resoluciones penales. Incorporación al Derecho español de los avances en cooperación judicial en la Unión Europea"* (MINECO, ref. DER 2015-63942-P).

2. La libre circulación tuvo su origen en el Tratado de Maastricht de 1992, pero tuvo su aplicación práctica con el Acuerdo de Schengen en 1995. Puede consultarse en: http://www.europarl.europa.eu/news/es/headlines/security/20180216STO98008/schengen-ampliacion-del-espacio-europeo-sin-fronteras-interiores

Las dificultades existentes para la persecución delictiva, y consiguiente incriminación del delincuente, se ven acrecentadas por la proliferación de los más modernos medios tecnológicos, potenciando nuevas formas de comisión de hechos delictivos a través de estos instrumentos tecnológicos, dotando de armas a los potenciales delincuentes y ampliando su campo de actuación, sin necesidad de desplazamiento físico para la realización de los mismos[3]. En este sentido, el Convenio de Budapest[4] señala la preocupación existente por que las redes informáticas y la información electrónica sean utilizadas por los potenciales delincuentes para la consecución de sus fines criminales.

Además, la tecnología ejerce un papel crucial en el intercambio de datos personales, traspasando, en algunas ocasiones, la esfera más íntima de la persona. Actualmente, existe una comercialización de los datos personales de los usuarios de internet, donde los entes comerciales trafican con esos datos y obtienen un beneficio como consecuencia de esa transmisión. Esta forma de operar, adquiere mayor relevancia cuando la comercialización se hace entre varias empresas con sede en diferentes países de la UE.

Ante la nueva realidad impuesta por las TICs, se hace necesario un control eficiente que salvaguarden los derechos e intereses fundamentales de los ciudadanos, así como la regulación de la transferencia de los datos personales que pueda favorecer la investigación y prevención delictiva por parte de las autoridades policiales y judiciales. Estamos, pues, ante el complejo binomio seguridad –desde el prisma de la prevención y persecución delictiva– y protección de los derechos fundamentales de investigados y/o acusados –derecho de protección a los datos personales–.

Con anterioridad a la entrada en vigor del Tratado de Lisboa, la normativa relativa a la protección de datos personales se encontraba fragmentada en en el primer pilar[5], referente a la protección de datos con fines privados y comerciales, y en el tercer pilar, referente a la protección de datos con fines de aplicación de la ley. Con la entrada en vigor del Tratado de Lisboa desapareció la estructura de los pilares, desarrollándose un sistema de protección de datos más compacto y eficaz.

En efecto, el derecho a la protección de datos de carácter personal de las personas físicas se encuentra recogido en la Carta de los Derechos Fundamentales de la UE (en adelante, CDFUE), en sus arts. 7 y 8, apdo.1, así como en el Tratado de Funcionamiento de la UE (en adelante, TFUE), en su art. 16, apdo.1. En el ordenamiento jurídico español se encuentra recogido en el art. 18 de la Constitución Española (en adelante, CE).

En el seno del Programa de la Haya de 2005 a 2010[6], la Comisión presentó una comunicación[7] donde se establecían diez prioridades, en el plazo de 5 años, en el Espacio

Europeo de libertad, seguridad y justicia (en adelante, ELSJ). Se pone de manifiesto la especial atención que hay que prestar a la protección de los datos personales, considerándose como un derecho con entidad propia, diferente al derecho a la intimidad. Concretamente en el apdo. 7 se hace referencia

3. En España, en el año 2017, se cometieron 81.307 ciberdelitos. En el año 2018, las Comunidades Autónomas con mayor índice de comisión de ciberdelitos fueron Andalucía, con una cifra que oscila los 15.458, Madrid, con 12.169, y Valencia, con 10.842. Información disponible en www.oedi.es
4. Convenio nº 185, del Consejo de Europa, de 23 de noviembre de 2001, sobre Ciberdelincuencia. España lo ha ratificado (BOE 17 de septiembre de 2010).
5. Los tres pilares lo conformaban: el pilar comunitario; el referido a la política exterior y de seguridad común; y el de cooperación policial y judicial en materia penal.
6. En materia penal, hay que destacar que el intercambio de datos personales ya se contempló en el Programa de Tampere (octubre 1999).
7. Comunicación de la Comisión al Consejo y al Parlamento Europeo, Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguri- dad y la justicia, COM 2005 184 final, 10 de mayo de 2005.

al complejo binomio *"derecho a la intimidad y seguridad en el intercambio de información",* siendo tarea de las autoridades policiales y judiciales lograr el equilibrio adecuado entre el derecho a la intimidad y la seguridad.

Posteriormente, el Consejo Europeo adoptó el Programa plurianual en el ámbito del ELSJ para el período 2010-2014 (Programa de Estocolmo)[8]. En las conclusiones del Consejo[9] se definieron las orientaciones estratégicas de la programación legislativa y operativa para los años siguientes en el ELSJ, contemplándose como objetivo, en la prevención y lucha contra la delincuencia y el terrorismo, la protección de los datos personales.

La regulación legislativa, hasta hace poco, se encontraba recogida en la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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[10] (en adelante, Directiva 95/46/CE); Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[11] (en adelante, Reglamento (CE) nº 45/2001); la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[12] (en adelante, Directiva 2002/58/CE); la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 , sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[13] (en adelante, Directiva 2002/24/CE); la Decisión Marco 2008/977/JAI sobre protección de datos personales tratados en el contexto de la cooperación policial y judicial en materia penal[14] (en adelante, DM 2008/977/JAI).

Actualmente, como consecuencia de las deficiencias existentes y de los cambios impuestos por las nuevas tecnologías, se ha promulgado la Directiva (UE) 2016/680, de 27 de abril de 2016, del Parlamento Europeo y del Consejo, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y sobre la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (en adelante, Directiva 2016/680/UE)[15]; y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ CE[16] (en adelante, RGPD).

8. Programa de Estocolmo "Una Europa abierta y segura que sirva y proteja al ciudadano", DO C 115 de 4 de mayo de 2010. Este Programa trae su origen en la comunicación que presentó la Comisión al Parlamento, titula- da "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos ", (COM 2009) 262 final, de 10 de junio de 2009.
9. EUCO 79/14, de 27 de junio de 2014.
10. DOUE L281, de 23 de noviembre de 1995.
11. DOUE L008, de 12 de enero de 2001.
12. DOUE L201/37, de 31 de julio de 2002.
13. DOUE L105/54, de 13 de abril de 2006.
14. DOUE L350/60, de 30 de diciembre de 2008.
15. DOUE L 119/89, de 4 de mayo de 2016.
16. DOUE L 119/88, de 4 de mayo de 2016.

1.- ASPECTOS GENERALES DEL REGLAMENTO (UE) 2016/679, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA A SUS DATOS PERSONALES Y LA LIBRE CIRCULACIÓN DE ESOS DATOS

El flujo de los datos personales del ciudadano es una cuestión que puede generar cierta inquietud sobre el tratamiento que se está dando a sus datos y la posible perdida de control de esos datos por parte del titular de los mismos. La *rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de datos personales*[17]*,* retos que requerían respuestas por parte del legislador europeo.

La Directiva 95/46/CE fue relevante en materia de protección de datos, la cual trató de armonizar, y aunque los objetivos y principios de la misma siguen siendo válidos[18], no es menos cierto que las diferencias en los niveles de protección de los derechos y libertades de las personas físicas hacían que existieran divergencias en la ejecución y aplicación de la Directiva 95/46/CE. Estas deficiencias hacen necesario un nivel uniforme y elevado de protección de estos derechos, que supere la fragmentación normativa, por ello, ha dado lugar a la promulgación del del RGPD.

La novedad estriba en que la regulación del derecho de protección de datos no se hace a través de una Directiva, sino a través de Reglamento, lo que significa que será directamente aplicable a los Estados miembros de la UE, sin necesidad de transposición[19]. El objeto del mismo es la protección de los derechos y libertades fundamentales de las personas físicas, en especial, el derecho a la protección de los datos personales. En España, recientemente se ha adaptado las disposiciones del RGPD al ordenamiento jurídico español, por medio de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[20] (en adelante, LOPDGDD). Un matiz que debemos hacer es la facultad que recae en los Estados miembros para establecer normas relativas al tratamiento de los datos personales de las personas fallecidas. España, ha sido uno de los países que ha dejado recogido el derecho a la protección de los datos personales de las personas fallecidas –art.3 LOPDGDD–, pudiendo ejercer estos derechos cualquier persona que tenga un vínculo familiar con la persona fallecida, si bien la disposición no establece límites en cuanto al grado de parentesco[21].

Respecto al ámbito de aplicación material, conviene precisar que el RGPD se aplicará al tratamiento total o parcial automatizado de datos personales, así como al tratamiento de datos no automatizados contenidos o destinados a ser incluidos en un fichero –art. 2–. Concretamente, no será de aplicación al tratamiento de datos personales que se efectúe por una persona física en el ejercicio de actividades que sean exclusivamente personales o domésticas. De igual modo, tampoco resultará de aplicación al tratamiento de los datos que se efectúe por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, resultando de aplicación, en el presente supuesto, la Directiva 2016/680/UE –art.1–, la cual abordaremos en el epígrafe siguiente.

Por otro lado, en cuanto al ámbito territorial, el RGPD se aplicará al tratamiento de datos personales

17. Considerando 6º del RGPD.
18. La Directiva fue derogada por el RGPD.
19. PLAZA PENADÉS, Javier, «El nuevo marco normativo de la protección de datos», en *Diario La Ley,* Sección Actualidad Civil, nº 5, mayo de 2018, Editorial Wolters Kluwer, pág. 8.
20. BOE núm. 294, de 6 de diciembre de 2018.
21. MUÑOZ RODRÍGUEZ, Joaquín, «Disposiciones generales. Título I (Arts. 1-5 RGPD. Arts.1-3 LOPDGDD)» en VVAA (coord. LÓPEZ CALVO, José) *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pág. 329.Considerando 32 del RGPD.

en el contexto de las actividades de un establecimiento del responsable o encargado en la UE, con independencia que el tratamiento tenga lugar en la UE o no –art. 3–.

Una cuestión que resulta de interés, y que ha marcado un hito con la promulgación del RGPD, es la prestación del consentimiento. Ésta difiere de la forma en que había de prestarse conforme a la Directiva 95/46/CE, pues la misma no exigía que el consentimiento se prestara de forma expresa, cuestión que el RGPD resuelve manifestando que el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre –por escrito o verbalmente–, por tanto, la intención del legislador europeo es que no exista ningún género de dudas en la prestación del consentimiento, no siendo posible la presentación del mismo de forma tácita[22].

Conforme a las condiciones para el consentimiento, dispone el art. 7 del RGPD que el responsable del tratamiento de los datos debe ser capaz de demostrar el consentimiento. También recoge la facultad del interesado de retirar el consentimiento en cualquier momento, circunstancia de la que debe ser informado.

Además, respecto al consentimiento prestado con anterioridad a la entrada en vigor del RGPD, el cual se prestó de forma diferente, aclara la nueva norma europea que cuando el consentimiento se haya otorgado de conformidad con la Directiva 95/46/UE no se exige que el interesado preste el consentimiento de nuevo si la forma de prestarlo se ajusta a las condiciones establecidas en el RGPD[23].

1.1.- LOS DENOMINADOS DERECHOS ARCO.

Los derechos ARCO han sido ampliados como consecuencia de la promulgación del RGPD, introduciéndose en el elenco de derechos: el derecho a la portabilidad, el derecho al olvido y el derecho a la limitación (derechos ARCOPOL). Éstos hacen referencia a aquellos derechos que pueden ser ejercitados, de forma personal, por el interesado.

1.1.1.- Derecho de acceso.

Con carácter preliminar, cabe recordar que el derecho de acceso, junto con el derecho de rectificación es uno de los derechos expresamente recogidos en el art. 8.2 de la CDFUE, lo cual denota la importancia de este derecho.

Este derecho se define como el derecho a acceder, por parte del interesado, a aquellos derechos que le conciernan[24]. Si bien este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluido los secretos comerciales o la propiedad intelectual y, en particular, a los derechos de propiedad intelectual que protegen programas informáticos. Esta garantía de la protección de los derechos de los terceros no debe operar de forma que ampare la negativa a prestar la información al interesado. Además, en base a la cantidad de información que opera en poder del responsable, se habilita al responsable para que pueda requerir al interesado para que especifique la información o actividades del tratamiento para la que cursa la solicitud –de acceso–.

Concretamente, este derecho de acceso está regulado en el art. 15 del RGPD, el cual establece que el interesado tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no los datos personales que le conciernen y, en dicho caso, acceso a los datos personales y a la siguiente información:

22. Considerando 117 RGPD.

23. El Considerando 63 del RGPD define el derecho de acceso como "*derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de co- nocer y verificar la licitud del tratamiento".*

24.

a). Los fines del tratamiento.

b). Categorías de los datos personales.

c). Los destinatarios o las categorías de destinatarios a los que se comunican los datos personales, en particular destinatarios en terceros u organizaciones internacionales.

d). El plazo de conservación de los datos personales o los criterios utilizados para fijar este plazo.

e). La existencia del derecho a solicitar del responsable la rectificación o supresión de los datos personales o la limitación del tratamiento de los datos personales relativos al interesado, o el derecho a la oposición.

f). Derecho a formular reclamación ante la autoridad de control.

g). Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen.

h). En el caso de existencia de decisiones automatizadas, incluida la elaboración de perfiles, tendrá derecho el interesado a conocer la información relativa a la lógica aplicada, así como la importancia y las consecuencias.

El mencionado precepto contempla la transmisión de datos personales a un tercer país o a una organización internacional, debiendo, en este supuesto, ser informado el interesado de las garantías adecuadas[25].

Asimismo, el apdo. 3 del art. 15 del RGPD recoge la obligación del responsable del tratamiento de facilitar una copia de los datos personales objeto del tratamiento al interesado. El RGPD faculta al responsable del tratamiento para fijar un canon razonable por las copias adicionales que se soliciten, sin embargo, no se establece esa facultad de fijar un canon para la primera copia que se solicite –siendo de carácter gratuito en virtud del art. 12.5 del RGPD–. Este canon –para copias adicionales (art. 15.3)– debemos diferenciarlo del establecido en el art. 12.5 del RGPD el cual faculta al responsable del tratamiento para cobrar un canon en el supuesto que las solicitudes sean infundadas o excesivas –siendo repetitivas–. El legislador español fija un plazo para considerar repetitivo el ejercicio del derecho de acceso, contemplando en el art. 13.3 de la LOPDGDD que "*a los efectos establecidos en el artículo12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello".* Por tanto, son dos situaciones diferentes[26].

Al mismo tiempo se establece la facultad de facilitar la información por formato electrónico cuando el interesado presente la solicitud por medios electrónicos y no requiera que la información se facilite de diferente modo.

1.1.2.- Derecho de rectificación.

Este derecho se encuentra recogido en el art. 16 del RGDP, regulándose, pues, el derecho de exactitud que tiene el interesado, donde se contempla la posibilidad que el interesado emita una solicitud de rectificación de los datos personales inexactos, solicitud que habrá de ser atendida por el responsable

---

25. Vid. art. 46.1 del RGPD.

26. PUYOL MONTERO, Javier, «Transparencia de la información y derecho de acceso de los interesados» en VVAA (Dir. RALLO LOMBARTE, Artemi) *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Tirant lo Blanch, Valencia, 2019, págs. 308 y ss.

del tratamiento de los mismos. Además, se añade la posibilidad de completar los datos que sean incompletos, incluso mediante una declaración adicional. Al respecto, se pronuncia APARICIO SALOM este derecho a completar los datos personales *"atribuye al interesado un derecho de disposición sobre el tratamiento*[27]*"*.

Contribuye a ampliar el precepto, el art. 14 de la LOPDGDD, donde se dispone que el afectado deberá indicar los datos concretos a los que se refiere y la corrección que haya de hacerse, obligando a aportar, cuando sea preciso, la documentación acreditativa de la inexactitud a la que se refiere.

Este derecho conecta directamente con los principios anunciados en el art. 5 del RGPD donde se proclama que los datos personales serán exactos y, en caso de resultar necesario, actualizados.

1.1.3.- Derecho de supresión (el anteriormente denominado Derecho de cancelación).

El derecho de supresión se encuentra recogido en el art. 17 del RGPD, en virtud del cual el interesado tendrá derecho a exigir, del responsable del tratamiento de los datos, la supresión de los datos personales. Se configura, así, como un derecho-obligación, tanto del interesado a formular la solicitud de supresión, como del responsable a suprimir los datos cuando concurra alguna de las siguientes circunstancias: que los datos no sean necesarios para los fines para los que fueron recogidos o tratados; que el interesado retire el consentimiento; que el interesado se oponga; que sean objeto de tratamiento ilícito; que la supresión traiga consecuencia en el cumplimiento de una obligación legal; que se hayan obtenido en relación con la oferta de servicios de la sociedad de información –en relación con la oferta de servicios realizada a niños y la consideración de licitud o ilicitud en función del umbral de edad–.

Conviene precisar que la LOPDGDD –art. 15 apdo. 2– introduce en este artículo, al regular el derecho de supresión, la derivación de la misma como consecuencia del ejercicio del derecho de oposición –en el supuesto de mercadotecnia directa–.

Como una manifestación del mismo, aparece el derecho al olvido en el apdo. 2 del art. 17 del RGDP, el cual trataremos en el epígrafe correspondiente.

1.1.4.- Derecho de oposición.

La regulación del mismo se hace en el art. 21 del RGPD –art. 18 de la LOPDGDD–. Podemos delimitar dos supuestos donde puede ejercerse este derecho: el primero de ellos, el enunciado en el Considerando 60, cuando concurra el supuesto que el tratamiento, lícito, de los datos sea necesario, salvo por razones de interés público o en ejercicio de los poderes públicos conferidos al responsable de los datos; el segundo, al que hace alusión el Considerando 70, cuando los datos sean tratados con fines de mercadotecnia directa. La consecuencia del ejercicio de este derecho es el cese en tratamiento por parte del responsable, con la excepción que se regula en el apdo.1 del art. 21, esto es, salvo que acredite motivos legítimos imperiosos para el tratamiento o para la formulación, el ejercicio o la defensa de las reclamaciones.

Exige el apdo. 4 del art. 21 del RGPD facilitar la información al interesado sobre este derecho en la primera comunicación que se efectúe.

27. APARICIO SALOM, Javier, «Derechos del interesado (Arts. 12-19 RGPD. Arts.11-16 LOPDGDD)» en VVAA (coord. LÓPEZ CALVO, José) *La adaptación al nuevo marco …*, *op.cit.* 345 y ss.

1.2.-DERECHO A LA PORTABILIDAD.

El derecho a la portabilidad se configura como uno de los nuevos derechos[28] introducidos por el art. 20 del RGPD –art. 17 de la LOPDGDD–. Mediante el ejercicio del mismo el interesado podrá solicitar del responsable del tratamiento que le devuelva los datos personales que le facilitó, o bien que se transmitan esos datos personales a otro responsable.

El ejercicio de este derecho encuentra su limitación en el art. 20. apdo. 3 cuando sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.

1.3.- DERECHO AL OLVIDO.

Al igual que el derecho del epígrafe anterior, este constituye una de las novedades del RGPD. La opción que opta el legislador europeo, en cuanto a su regulación, es incluirlo dentro del art. 17 –apdo.2– del RGPD junto con el derecho de supresión.

En efecto, se configura como una manifestación del derecho de supresión, en el sentido de informar a los responsables que estén tratando datos personales del interesado de la solicitud de supresión de cualquier enlace a esos datos, o cualquier copia o réplica, si bien, el matiz radica, aquí, en la publicación de los datos, momento en que se podrá ejercitar el derecho.

Se establecen limitaciones al derecho de supresión, así como al derecho al olvido, no pudiendo ejercerse ambos derechos cuando concurran los supuestos detallados en el apdo.3 del art. 17 del RGPD.

1.4.- DERECHO A LA LIMITACIÓN.

Este derecho se regula en el art. 18 del RGPD, en virtud del cual el interesado tendrá derecho a obtener del responsable la limitación del tratamiento cuando se den los requisitos que se enumeran en el precepto.

Se establece una excepción al mismo, que es la dispuesta en el apdo. 2 del art. 18 del RGPD, habilitándose para ser objeto de tratamiento, con el consentimiento del interesado o para la formulación, el ejercicio o la densa de reclamaciones u orientado a la protección de los derecho de otra persona.

El precepto impone la obligación de información al interesado antes que proceda el levantamiento de la limitación, para el supuesto que se haya acordado la misma.

2.- PRINCIPIO DE DISPONIBILIDAD Y PROCESO PENAL EN EL MARCO DE LA DIRECTIVA (UE) 2016/680, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, RELATIVA A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES POR PARTE DE LAS AUTORIDADES COMPETENTES PARA FINES DE PREVENCIÓN, INVESTIGACIÓN, DETECCIÓN O ENJUICIAMIENTO DE INFRACCIONES PENALES O DE EJECUCIÓN DE SANCIONES PENALES, Y A LA LIBRE CIRCULACIÓN DE DICHOS DATOS.

III.1.- EL PRINCIPIO DE DISPONIBILIDAD Y SU DESARROLLO LEGISLATIVO EN EL ÁMBITO PENAL.

Como consecuencia de los trágicos ataques terroristas, concretamente los atentados de Nueva York, Madrid y Londres, se hizo necesario mejorar el sistema de transmisión de datos entre los Estados miembros para la erradicación de la lacra del terrorismo, así como la adopción de medidas que reforzara la cooperación policial. La conmoción por los atentos acaecidos llevaron a que el Consejo apro-

28. Sobre estos nuevos derechos *Vid.* Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre "mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Regla- mento general de protección de datos a partir del 25 de mayo de 2018", COM (2018) 43 final, de 24 de mayo de 2018.

bara la Declaración sobre la lucha contra el terrorismo –en 2004–[29], donde se ponía el foco de atención, entre otras medias, en la simplificación del intercambio de información entre los cuerpos y fuerzas de seguridad de los Estados miembros. Ese mismo año, la Comisión presentó sendas Comunicaciones, en mayo tuvo lugar una, para *"reforzar la cooperación policial y aduanera en la Unión Europea"*[30] y, en junio, la otra "*sobre la mejora del acceso a la información por parte de las autoridades encargadas de garantizar el cumplimiento de la ley"*[31].

En la primera de las comunicaciones se considera que la ampliación de la UE –consecuencia de la integración de nuevos Estados miembros– hace necesario clarificar y establecer prioridades para la cooperación aduanera y policial de cara al futuro. En sus conclusiones y recomendaciones se señalan dos grandes ejes de actuación para mejorar la cooperación policial y aduanera: el primero de ellos, el referido al flujo de información[32]; el segundo, la efectiva cooperación transfronteriza.

La segunda de ellas, proclama la libre circulación de la información entre EUROPOL y EUROJUST e introduce el *principio de acceso equivalente*, mediante el cual se permitía a las autoridades y funcionarios encargados de garantizar el cumplimiento de la ley –esto es, autoridades policiales– pudieran acceder a las bases de datos de otros Estados miembros, como si fuera una base de datos propia de las autoridades y funcionarios nacionales competentes.

Finalmente, se desarrolló el *principio de disponibilidad*, recogiéndose expresamente en el Programa de la Haya de 2005 a 2010, conforme al cual las autoridades competentes de cada Estado miembro podrán acceder a los datos personales en orden a la prevención e investigación de delitos[33].

Un hito relevante en el inicio del desarrollo del principio de disponibilidad fue el acontecido con el Tratado de Prüm[34], estableciéndose la intención de reforzar la cooperación transfronteriza y, en especial, el intercambio de información –en clara referencia al principio de disponibilidad–[35].

---

29. Declaración de Bruselas, de 25 de marzo de 2004. Se manifestó 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 deli- tos 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 se- guridad de los Estados miembros".*

30. Comunicación de la Comisión al Parlamento Europeo y al Consejo para reforzar la cooperación policial y aduanera en la Unión Europea, de 18 de mayo de 2004, COM (2004) 376 final.

31. Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre la mejora del acceso a la información por parte de las autoridades encargadas de garantizar el cumplimiento de la ley, de 16 de junio de 2004, COM (2004) 429 final

32. *Cfr.* COM (2004) 376….*op.cit.* págs. 40 y ss. Concretamente señala la necesidad de *"garantizarse la interope- rabilidad de las diferentes bases de datos y sistemas de comunicación, tanto policiales como aduaneros, utiliza- dos por los servicios responsables de la aplicación de las leyes de los Estados miembros. Al nivel institucional de la UE, habría que hallar mecanismos para fomentar la colaboración y el intercambio de datos entre la OLAF y Europol. Debería concluirse un acuerdo que regulara el intercambio de datos personales entre ambos".*

33. GALÁN MUÑOZ, Alfonso, «La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea» en VVAA (Dir. COLOMER HERNÁNDEZ, Ignacio) *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea",* Aranzadi, Cizur Menor, 2015, págs. 37 y ss.

34. El 27 de mayo de 2007 siete Estados miembros (Bélgica, Alemania, España, Francia, Luxemburgo, Holanda y Austria; posteriormente suscrito por Italia, Finlandia, Portugal, Bulgaria, Hungría, Rumanía, Eslovaquia y Eslo- venia) firmaron el Convenio relativo a la profundización de la cooperación transfronteriza, en particular en mate- ria de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal.

35. DE HOYOS SANCHO, Montserrat, «Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos», en VVAA (Dir. ARANGÜENA FANE- GO, Coral) *Espacio europeo de libertad, seguridad y justicia: últimos avances en cooperación judicial penal,* Lex Nova, Valladolid, 2010, págs. 151 y ss. Afirma la autora que *"el Tratado de Prüm supuso en su momento un hito en el reforzamiento*

A iniciativa sueca, tuvo origen la Decisión Marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea[36] (en adelante, DM 2006/960/JAI), considerada, por algunas voces reconocidas, como una primera aproximación del principio de disponibilidad[37]. Entre sus objetivos, se encuentra la necesidad de establecer normas que permitan el intercambio, entre los servicios de seguridad de los Estados miembros, rápido y eficaz de información e inteligencia disponibles para llevar a cabo investigaciones criminales, velando por la protección de los datos personales.

Posteriormente, en aras de desarrollar el principio de disponibilidad y con el objeto de implementación del Tratado, se promulgó la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza[38], con el objetivo de incorporar los aspectos esenciales de las disposiciones de dicho Tratado en el ordenamiento jurídico de la UE. La Decisión 2008/615/JAI contemplaba entre sus disposiciones: por un lado, el acceso a los ficheros de análisis de ADN[39], así como a los sistemas automatizados de identificación dactiloscópica; y, por otro lado, la consulta automatizada de los datos de registros de matriculación de vehículos. De igual modo, se introducen disposiciones relativas a la transmisión de datos con el objetivo de prevenir ataques terroristas, así como disposiciones encaminadas a reforzar la cooperación policial, con fines de prevención de delitos y amenazas para la seguridad y el orden público. En consecuencia, la novedad radica aquí en el acceso en línea para la consulta de las bases de datos de otros Estados miembros[40].

Finalmente, debemos reseñar la Decisión 2008/616/JAI del Consejo, de 23 de junio de 2008, 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[41], la cual tiene como objetivo la ejecución de la Decisión Prüm[42].

Continuando con el afán de seguir desarrollando el ELSJ, y con la imperante preocupación de los atentados terroristas, en el Programa de Estocolmo 2010-2014 se establecen las prioridades para llevar a cabo en los años venideros, entre ellas, la protección de los derechos fundamentales de los ciudadanos, en especial el derecho de protección de datos de carácter personal. También, se pone de manifiesto

---

y profundización de la cooperación transfronteriza entre las autoridades encargadas de la persecución penal en los respectivos Estados firmantes de aquél".

36. DOUE L386, de 29 de diciembre de 2006.

37. MARTÍNEZ PÉREZ, Fernando y POZA CISNEROS, María, «El principio de disponibilidad: antecedentes penales y convenio de Prüm» en VVAA (Dir. CARMONA RUANO, Miguel, GONZÁLEZ VEGA, Ignacio U., MORENO CATENA, Víctor) *Cooperación Judicial Penal en Europa,* Madrid, Dykinson, 2013, págs. 417 y ss

38. DOUE L210, de 6 de agosto de 2008.

39. Cfr. DE HOYOS SANCHO, Montserrat, «Profundización en la cooperación transfronteriza en la Unión Euro- pea… », *op. cit.* págs. 151 y ss. Al respecto manifiesta la autora que *"el sistema general previsto en la Decisión […] dejando bien claro que no está prevista en la norma la posibilidad de un acceso directo de las autoridades encargadas de la persecución penal a todos los datos de los respectivos ficheros nacionales de perfiles de ADN. El mecanismo de intercambio de información se ha diseñado de tal manera que se pueda saber con rapidez y certeza si el dato que se busca […] se encuentra o no se encuentra archivado en la base o base de datos nacio- nales consultadas".*

40. GONZÁLEZ CANO, María Isabel, «Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial penal en la Unión Europea», en VVAA (Dir. COLOMER HERNÁNDEZ, Ignacio) *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios,* Aranzadi, Cizur Menor, 2017, págs. 41 y ss.

41. DOUE L210, de 6 de agosto de 2008.

42. En España, la regulación referente a la materia reseñada se encuentra en la LO 10/2007, de 8 de octubre, regu- ladora de la base de datos policial sobre identificadores obtenidos a partir del ADN; así como en los arts. 326, 363 y 778.3 de la LECRIM.

los logros conseguidos a través de los instrumentos creados para recabar, procesar y compartir información entre autoridades nacionales y otros actores europeos, contribuyendo el principio de disponibilidad a dar impulso a esta labor. En este orden de cuestiones, el citado Programa contempla la necesidad de realizar un estudio de viabilidad para la creación de un Sistema Europeo de Fichero Policial (EPRIS), así como un sistema de registros de nombres de pasajeros (PNR)[43], a efectos de prevención, detección, investigación y enjuiciamiento de los delitos terroristas y los delitos graves.

La consagración del principio de disponibilidad, como afirma GONZÁLEZ CANO[44], viene dada por la DM 2008/977/JAI. Como se dispone en su art.1, el objeto de la misma es 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. Igualmente, se procedió a la regulación del tratamiento posterior de los datos cedidos, así como su conservación y posterior transmisión a particulares. En definitiva, viene a establecer un cuerpo de normas comunes del tratamiento de los datos personales en el marco de la cooperación policial y judicial penal.

No obstante, debemos detenernos brevemente en los motivos por los cuales la DM 2008/977/ JAI no funcionó ni llegó a consagrarse como norma de referencia en esta materia. En primer lugar, su ámbito de aplicación era limitado, ya que su extensión se circunscribía al intercambio de datos personales entre diferentes Estados, pero no se hacía referencia al intercambio de datos en el ámbito nacional –entre autoridades de un mismo Estado–. En segundo lugar, tampoco se mostró una regulación armonizada que paliara las diferencias existentes entre los Estados miembros. Por último, se daba la ausencia absoluta del principio de especialidad y, además, se daba la circunstancia que el art. 3.2 de la DM 2008/977/JAI, en concordancia con el art. 11, admitía la utilización de datos para fines distintos de los que originaron la transmisión de los mismos, siempre que concurrieran los siguientes requisitos:

a) que no sea incompatible con los fines para los que se recogieron los datos; b) las autoridades competentes estén autorizadas a tratar los datos para tales otros fines; c) el tratamiento sea necesario para ese otro fin y proporcionado a él.

Lo que viene a ponerse de manifiesto es que estas excepciones al principio de especialidad permiten un tratamiento para cualquier otro fin diferente para el que se obtuvieron los datos.

En este sentido, se pronuncia GONZÁLEZ CANO afirmando que *"esta posibilidad de que el Estado cesionario utilice los datos obtenidos para otros fines y para la investigación y enjuiciamiento de otros delitos, directamente relacionados o no con aquellos para cuya investigación y enjuiciamiento se cedieron, aunque parece responder al principio de proporcionalidad y necesariedad, sin embargo desconoce el principio de especialidad, lo que conlleva un grave déficit de garantías para el sujeto sospechoso o acusado, y, además, puede dar lugar a graves reticencias por parte del Estado cedente"*[45].

43. Directiva 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuicia- miento de los delitos de terrorismo y de la delincuencia grave, DOUE L119, de 4 de mayo de 2016.

44. Cfr, GONZÁLEZ CANO, María Isabel, «Cesión y tratamiento de datos personales, principio de disponibili- dad…», *op.cit.* 41 y ss.

45. Cfr, GONZÁLEZ CANO, María Isabel, «Cesión y tratamiento de datos personales, principio de disponibili- dad…», *op.cit.* 41 y ss.

2.2.- PRINCIPIOS RECTORES DE LA OBTENCIÓN Y EL TRATAMIENTO DE DATOS PERSONALES EN LA DIRECTIVA (UE) 2016/680.

Ante las deficiencias normativas que existían y con la imperiosa necesidad de dar respuestas a las exigencias producidas por el desarrollo tecnológico, se promulgó la Directiva 2016/680/ UE[46]. Con el objetivo marcado de fortalecer el ELJS, resulta necesario facilitar la libre circulación de datos personales entre las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento en el ámbito de la cooperación penal[47].

El objeto de la misma es establecer normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes, a efectos de prevención, investigación, detección y enjuiciamiento[48].

Los principios rectores del tratamiento de los datos personales se recogen en el art. 4.1 de la Directiva 2016/680/UE considerando que los datos personales deberán ser:

a). tratados de manera lícita y leal;

b). recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;

c). adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados;

d). exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados;

e). conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados; f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas.

En el apdo. 2 del art. 4 de la Directiva 2016/680/UE, para los fines establecidos en apdo. 1 del art.1 –esto es, fines de prevención, investigación, detección o enjuiciamiento– se permite el tratamiento autorizado de dichos datos para fines distintos de aquel para el que se recojan, siempre que el responsable del tratamiento esté autorizado, y con sujeción a los principios de necesidad y proporcionalidad. En definitiva, la excepción al precepto general viene marcada por este apdo., el cual prevé la posibilidad que se traten los datos para el mismo fin pero en distinta causa, siempre y cuando el tratamiento esté autorizado para fines distintos; ello opera, como una excepción al principio de especialidad.

---

46. Así queda recogido en el Considerando 3º de la Directiva 2016/680/UE: *"La rápida evolución tecnológica y la globalización han planteado nuevos retos en el ámbito de la protección de los datos personales. Se ha incre- mentado de manera significativa la magnitud de la recogida y del intercambio de datos personales. La tecnolo- gía permite el tratamiento de los datos personales en una escala sin precedentes para la realización de activida- des como la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales".*

47. Considerando 4º de la Directiva 2016/680/UE.

48. Respecto a su ámbito de aplicación establece el Considerando 14 que "p*uesto que la presente Directiva no debe aplicarse al tratamiento de datos personales en el marco de una actividad que no esté comprendida en el ámbito de aplicación del Derecho de la Unión, no deben considerarse comprendidas en el ámbito de aplicación de la presente Directiva las actividades relacionadas con la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional y las actividades de tratamiento de datos personales que lleven a cabo los Estados miembros en el ejercicio de las actividades incluidas en el ámbito de aplicación del título V, capítulo 2, del Tratado de la Unión Europea (TUE)".*

Por otro lado, los derechos del interesado se regulan en el capítulo III de la Directiva 2016/680/UE– arts. 12 a 18–. Concretamente, el responsable del tratamiento de los datos tendrá la obligación de informar al interesado de la información contenida en el at. 13 apdo. 1 de la Directiva 2016/680/UE, si bien, tal derecho puede verse limitado al amparo de lo dispuesto en el art. 13 apdo. 3 al prever que los Estados miembros adopten medidas legislativas por las que se retrase, limite u omita la puesta a disposición del interesado de la información contenida en el apdo. 2 –información adicional–[49]. Esta posibilidad requiere que la medida sea necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada para: a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; c) proteger la seguridad pública; d) proteger la seguridad nacional; e) proteger los derechos y libertades de otras personas.

El precepto hace recaer la facultad de limitación del derecho a la información en los Estados miembros, con los diferentes criterios que se puedan adoptar en cada Estado miembro, careciendo de un cierto grado de precisión. De igual modo, el precepto no contempla plazos máximos para la limitación del derecho, que como argumenta GONZÁLEZ CANO *"no establecer ninguna regla sobre duración de estas limitaciones no es una opción muy respetuosa con el principio de proporcionalidad[50]"*.

El derecho de acceso, regulado en el art. 14 de la Directiva 2016/680/UE, establece el derecho del interesado a obtener, del responsable del tratamiento, confirmación de si se están tratando o no sus datos personales y, en caso afirmativo, el acceso a dichos datos. Este derecho puede verse limitado al amparo de las causas establecidas en el art. 15 de la Directiva 2016/680/UE, con sujeción a los principios de proporcionalidad y necesidad. Al igual que sucede en la limitación del derecho de información, en la limitación del derecho de acceso tampoco se fijan plazos de duración de la medida limitativa, lo que podría conllevar a una limitación que se dilate en el tiempo.

Hay autores que sostienen el carácter controvertido de estos derechos, dada la existencia de reconocimiento de los derechos procesales al sospechoso o acusado en el marco del proceso penal, pues ya tienen reconocidos el derecho a ser informados sobre la acusación, el derecho a defenderse, así como el acceso a las actuaciones. GUTIÉRREZ ZARZA considera que *"no es preciso reconocerles sus equivalentes en materia de protección de datos, esto es, los derechos de información y acceso[51]"*. A nuestro juicio, entendemos que la información de los derechos en materia de protección de datos supone un plus a las garantías de los sospechosos o acusados, pues si bien es cierto que en el marco del proceso el sospechoso o acusado tiene reconocidos ya los derechos procesales, no es menos cierto que los derechos recogidos por la Directiva 2016/680/UE –los relativos a la información y acceso– van orientados, por ejemplo, a informar al interesado de su derecho a presentar una reclamación ante

49. Art. 13.2 Directiva 2016/680/UE: "*Además de la información indicada en el apartado 1, los Estados miem- bros dispondrán por ley que el responsable del tratamiento de los datos proporcione al interesado, en casos concretos, la siguiente información adicional, a fin de permitir el ejercicio de sus derechos: a) la base jurídica del tratamiento; b) el plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo; c) cuando corresponda, las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales; d) cuando sea necesario, más información, en particular cuando los datos personales se hayan recogido sin conocimiento del interesado"*.

50. Cfr: GONZÁLEZ CANO, María Isabel, «Cesión y tratamiento de datos personales, principio de disponibili- dad…», *op.cit.* 41 y ss.

51. GUTIÉRREZ ZARZA, Ángeles, «La protección de las personas físicas en lo que respecta a su derecho a la intimidad y los datos personales por las autoridades de emisión y ejecución de las órdenes europeas de investiga- ción» en VVAA (Dir. ARANGÜENA FANEGO, Coral y DE HOYOS SANCHO, Montserrat) *Garantías proce- sales de investigados y acusados. Situación actual en el ámbito de la Unión Europea,* Tirant lo Blanch, Valencia, 2017, págs. 435 y ss.

la autoridad de control, el derecho a solicitar del responsable del tratamiento su rectificación o supresión, etc. Por ello, el sospechoso o acusado no es informado de estas cuestiones al proporcionársele la información sobre sus derechos procesales. Esta cuestión afianza la necesidad de transposición de la citada Directiva en el ordenamiento jurídico español

Continúa el art. 16 de la Directiva 2016/680/UE con el derecho de rectificación o supresión de datos personales, otorgándose el derecho al interesado de rectificar los datos inexactos o a completar aquellos que estén incompletos, en particular, mediante una declaración suplementaria. El apdo. 6 del art. 16 de la Directiva 2016/680/UE viene a establecer una similitud con el art. 17.2 RGPD –derecho al olvido–, disponiendo la notificación al destinatario de los datos personales que hayan sido rectificados o suprimidos, o se haya limitado el tratamiento, para que aquél proceda a la rectificación, supresión o limitación del tratamiento.

Por último, el art. 18 de la Directiva 2016/680/UE da por finalizado el capítulo III, con los derechos del interesado en las investigaciones y los procesos penales, haciendo recaer en los Estados miembros la facultad para disponer de los derechos mencionados *ut supra* – información, acceso, rectificación o supresión– conforme al Derecho del Estado en cuestión.

Ya en el Capítulo VIII, el art. 52 de la Directiva 2016/680/UE reconoce el derecho del interesado a presentar una reclamación ante una autoridad de control si se ha producido vulneración de las disposiciones de la citada Directiva. Sigue el art. 53 de la Directiva 2016/680/UE con el derecho a la tutela judicial efectiva contra una resolución jurídicamente vinculante emanada de una autoridad de control[52].

En base a la normativa detallada, y con los argumentos expuestos, queda claro que se debe conseguir el equilibrio entre la protección de los derechos fundamentales de los ciudadanos y combatir las formas de delincuencia que siguen proliferando en el ámbito de la UE. Ahora bien, quizás debamos reflexionar, si como fundamento basado en la lucha contra la delincuencia –especialmente, los actos terroristas y formas similares de delincuencia grave– los ciudadanos no estamos, cada vez, más sometido a un control y seguimiento de nuestros datos personales –v.gr. datos PNR–[53].

2.3.-EL CAMINO MARCADO POR LA JURISPRUDENCIA DEL TJUE.

La jurisprudencia del TJUE ha sido decisiva en las nuevas orientaciones seguidas por la normativa vigente –Directiva 2016/680/UE–. Especial consideración hay que hacer a las sentencias dictadas por este tribunal: en primer lugar, la STJUE, de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12, que tiene su origen en peticiones de cuestiones prejudiciales planteadas por Irlanda y Austria[54]; en segundo lugar, la STJUE, de 21 de diciembre de 2016, en los asuntos acumulados

52. PILLADO GONZÁLEZ, Esther, «Difícil equilibrio entre seguridad y salvaguarda del derecho a la protección de datos personales en la prevención, investigación y represión de delitos en la Unión Europea» en VVAA (Dir. GONZÁLEZ CANO, María Isabel) *Integración europea y justicia penal,* Tirant lo Blanch, Valencia, 2018, págs. 515 y ss.

53. GALÁN MUÑOZ, Alfonso, «Los nuevos instrumentos de prevención y lucha contra el nuevo terrorismo: malas noticias para la intimidad y otros derechos fundamentales» en VVAA (Dir. COLOMER HERNÁNDEZ , Ignacio) *Cesión de Datos Personales y Evidencias entre Procesos Penales ... op.cit.* págs. 81 y ss. Expone el autor que *"los derechos fundamentales de los ciudadanos están siendo sometidos a enormes tensiones y restric- ciones en los últimos tiempos como consecuencia de un fenómeno criminal muy concreto: el denominado terro- rismo yihadista […]. La conclusión es desalentadora, pero no puede ser otra. Corren malos tiempos para los derechos fundamentales y es por ello, por lo que, hoy más que nunca, hay que recordar que la política criminal de los países democráticos no puede estar exclusivamente orientada a la efectividad en la prevención y castigo de delitos, sino que también ha de tender a garantizar los derechos y garantías que los convierten tales".*

54. Tribunal de Justicia de la Unión Europea, Gran Sala, Sentencia de 8 de abril de 2014, asunto C-293/12 y C−594/12. Disponible en: www.curia.europea.eu

C-203/15 y C-698/15, que tiene su origen en peticiones de cuestiones prejudiciales planteadas por Suecia y Reino Unido[55]; y, por último, la STJUE, en el asunto C-207/16, que tiene su origen en las cuestión prejudicial planteada por la AP de Tarragona[56].

En la STJUE de 8 de abril de 2014, la cuestión principal versa sobre la validez de la Directiva 2006/24/CE y su compatibilidad con los derechos a la vida privada y la protección de los datos de carácter personal, así como a la libertad de expresión (arts. 7, 8, 11 CDFUE). La cuestión trataba sobre si la conservación por los proveedores de los datos personales conllevan una colisión con los derechos fundamentales de los arts. 7 y 8 de la CDFUE.

El TJUE establece que aunque la conservación de datos que impone la Directiva 2006/24/CE constituye una injerencia en el derecho fundamental a la protección de datos de carácter personal y en el derecho a la vida privada, no permite la revelación del contenido de las comunicaciones. Si bien, partiendo de la premisa que la injerencia responde a un objetivo de interés general, considera que la injerencia encuentra legitimación en la valiosa información que se puede obtener de los datos conservados para la investigación, detección y enjuiciamiento –teniendo como finalidad la lucha contra la delincuencia organizada y la seguridad–.

Analizando en profundidad, la Directiva 2006/24/CE considera el TJUE que: en primer lugar, el campo de aplicación de la misma es extenso, sin que se establezca limitación, pues se aplica a todos los usuarios registrados o abonados, a todos los medios de comunicación electrónica y datos; igualmente, se aplica a todas las personas, incluso aquellas sobre las que no exista indicio o sospecha de la comisión de un hecho delictivo grave; en segundo lugar, tampoco establece ningún criterio para delimitar el acceso y utilización a los datos por las autoridades competentes; en tercer lugar, fija un período mínimo de seis meses para la conservación de los datos, pero no establece distinción entre las categorías de datos previstas en función con la utilidad que va a reportar al objeto perseguido o a los afectados.

En base a ello, considera el TJUE que la Directiva 2006/24/CE constituye una injerencia en los derechos fundamentales, no respetándose por el legislador el principio de proporcionalidad, siendo esto motivo suficiente por el que se declaró la invalidez de la Directiva 2006/24/CE.

Por otro lado, otra de las sentencias relevantes dictadas por el TJUE es la de 21 de diciembre de 2016, la cual tiene por objeto la interpretación del art. 15 apdo. 1 de la Directiva 2002/58/ CE en relación con los arts. 7, 8 y 52.1 de la CDFUE. La problemática dimana de la invalidez de la Directiva 2006/24/CE y la no conservación de los datos por parte de los proveedores de servicio objeto del litigio, hecho que fue notificado por la empresa Tele2. Sin embargo, el Derecho sueco si establecía la obligación de conservación de esos datos, por tanto, se suscita la controversia en relación a la compatibilidad con el Derecho de la UE. Por oro lado, los Sres. Watson, Brice y Lewis –asunto C-698/15– presentaron recursos por los que solicitaban el control de la legalidad del art. 1 de la DRIPA, invocando en particular la incompatibilidad de dicho artí. con los arts. 7 y 8 de la Carta y con el art. 8 del CEDH. La Court of Appeal (England & Wales) decidió suspender el procedimiento y plantear cuestión prejudicial ante el TJUE. El TJUE resolvió ambas cuestiones prejudiciales concluyendo que, en consonancia con los argumentos utilizados en en la Sentencia de 8 de abril de 2014, considera que el art. 15. apdo.1 de la Directiva 2002/58/UE, en relación con los arts. 7, 8 y 52.1 CDFUE se opone a una normativa nacional: de un modo, *"que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos*

55. Tribunal de Justicia de la Unión Europea, Gran Sala, Sentencia de 21 de diciembre de 2016, asunto C203/15 y 698/15. Disponible en: www.curia.europea.eu

56. Tribunal de Justicia de la Unión Europea, Gran Sala, Sentencia de 2 de octubre de 2018, asunto C-207/16. Disponible en: www.curia.europea.eu

los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica"; de otro; "*que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión".* Por último, el TJUE consideró inadmisible la segunda cuestión prejudicial planteada por la Court of Appeal (England & Wales).

En última instancia, la STJUE de 2 de octubre de 2018 tiene por objeto la interpretación del art. 15.1 de la Directiva 2002/58/CE en relación con los arts. 7 y 8 de la CDFUE. El procedimiento principal, que, posteriormente, derivó en la presente cuestión prejudicial, traía causa en una denuncia presentada ante la Policía como consecuencia de un robo con violencia, donde se sustrajo, entre otras cosas, el teléfono móvil del denunciante. Con objeto de averiguar los sujetos responsables del hecho delictivo, la Policía solicitó que se se ordenara a diversos proveedores la transmisión de datos personales en aras a la identificación de los titulares de las tarjetas SIM activadas con el teléfono móvil sustraído, resultando la diligencia denegada por el juez instructor[57]. En el supuesto de hecho la cuestión se circunscribe a si la gravedad del delito cometido es suficiente para habilitar a la obtención de los datos personales conservados por los proveedores de servicios, con clara injerencia en los derechos fundamentales. Al respecto considera el TJUE que la injerencia en los derechos fundamentales de los individuos no reviste el carácter de gravedad, en base a que con los datos obtenidos a través de las tarjetas SIM no se puede conocer la fecha, la hora, la duración , el lugar o los destinatarios de las comunicaciones efectuadas con esas tarjetas, por tanto, no permiten extraer conclusiones precisas sobre la vida privada de los afectados. Por los motivos expuestos, concluye el TJUE que la injerencia en los derechos fundamentales está justificada con fundamento en la prevención, investigación, descubrimiento y persecución delictiva.

2.4.- BREVE CONSIDERACIÓN SOBRE DISPONIBILIDAD DE DATOS PERSONALES Y ORDEN EUROPEA DE INVESTIGACIÓN.

En el actual marco de la cooperación judicial penal, ha supuesto un nuevo planteamiento, que surge con ánimo de ser más ambicioso que los instrumentos anteriores, la Directiva 2014/41/ UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal[58] (en adelante, DOEI). La Directiva 2014/41/UE supone un nuevo esquema normativo donde se unifica en un sólo instrumento las normas comunes para la obtención de pruebas[59]. En España, se ha transpuesto la DOEI mediante la Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea (en adelante, LRMRP).

Se contempla expresamente, en su considerando 40, la protección de los datos personales: *"La pro-*

57. El auto se deniega en virtud de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las co- municaciones electrónicas y a las redes públicas de comunicaciones, la cual limita la cesión de los datos conser- vados por las operadoras de telefonía móvil a los delitos graves. Posteriormente entró en vigor la LO 13/2015, que como expone el tribunal, introduce dos criterios para determinar la gravedad del delito: por un lado, el com- puesto por conductas típicas de especial relevancia; y, por otro lado, que la pena prevista para el delito en cues- tión supere el umbral de tres años.

58. DOUE 130, de 1 de mayo de 2014.

59. Se deroga la Decisión Marco 2008/978/JAI del Consejo, de 18 de diciembre de 2008, relativa al exhorto euro- peo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal.

tección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. De conformidad con el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del TFUE, toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

Asimismo, en el considerando 42 se hace referencia al uso de los datos personales cuando obedezcan a los principios de necesidad y proporcionalidad, disponiéndose lo siguiente: *"Los datos personales obtenidos en virtud de la presente Directiva deben procesarse solo cuando sea necesario y ser proporcionados para fines compatibles con la prevención, investigación, detección y enjuiciamiento de delitos, la aplicación de sanciones penales y el ejercicio de los derechos de la defensa. Solo personas autorizadas deben tener acceso a información que contenga datos de carácter personal que puedan conseguirse a través de procesos de autenticación"*. De este modo, el artículo 20 de la DOEI hace una remisión a la DM 2008/977/JAI, derogada por la Directiva 2016/680/UE, por tanto, ésta última será de aplicación al tratamiento de los datos personales.

Del mismo modo, la LRMRP, al transponer la DOEI, dedica el art. 193 a la utilización de los datos personales obtenidos en la ejecución de una OEI en otro Estado miembro, esto significaría que España ocuparía la posición de Estado de emisión. Dispone el precepto que los datos que se obtengan como consecuencia de la ejecución de una OEI *sólo podrán ser empleados en los procesos en los que se hubiera acordado la resolución.* Hasta este punto parece acertado el precepto, pues, lo que viene a decir es que los datos obtenidos sólo podrán utilizarse en el marco del proceso para el que se emitió la OEI. Pero el precepto no finaliza aquí, continúa el mismo, con un marcado carácter de imprecisión, disponiendo que los datos obtenidos podrán ser empleados en *aquellos otros relacionados de manera directa con aquél o excepcionalmente para prevenir una amenaza inmediata y grave para la seguridad pública.* Esto viene a suponer el establecimiento de dos excepciones al principio de especialidad, que vienen a proclamar que la medida de investigación que se adopte sea para un delito concreto, finalidad que resulta mermada con el establecimiento de estas excepciones. Dicho sea de paso, el principio de especialidad no queda expresamente regulado ni en la DOEI ni en la LRMRP.

A.- Dicho esto, ¿qué debemos entender por "amenaza grave e inmediata"?.

Esta excepción al principio de especialidad, también queda recogida en la Directiva 2016/680/ UE. Así, pues, se contempla la posibilidad de transmisión de datos personales a otro Estado miembro o a un tercer país, a los fines establecidos en el apdo.1 del art.1, sin necesidad de autorización previa en el supuesto de amenaza inmediata y grave para la seguridad pública – art. 35.2 de la Directiva 2016/680/UE–. Y, además, amparados en esta "amenaza" el art. 13 de la Directiva 2016/680/UE establece una restricción para los derechos de investigados y/o acusados, pues contempla la posibilidad de limitar el derecho de acceso, información, supresión y rectificación sin fijar plazo máximo de limitación de dichos derechos, todo ello, en aras de proteger la seguridad pública y nacional. Por tanto, establecer una excepción al principio de especialidad bajo la máxima de la "amenaza inmediata y grave para la seguridad pública", contemplando la posibilidad de limitar los derechos mencionados, tiene el riesgo que esas limitaciones se perpetúen en el tiempo, lo cual no parece muy coherente con el respeto a los derechos y garantías de investigados y/o acusados.

B.- Y con respecto a la otra excepción ¿qué debemos entender por otro proceso relacionado de manera directa con aquél en el que se adoptó la OEI?

En este punto, resulta necesario traer a colación el supuesto de hallazgo o descubrimiento casual, el cual ha sido tratado por la jurisprudencia, así como recogido en la LECRIM en sus arts. 579 bis y 588 bis i). Esto supone, el hallazgo de nuevos elementos probatorios, relacionados con otro delito o persona

distinta, en el seno de una investigación de un delito concreto. No obstante, consideramos que el efecto del hallazgo casual puede extenderse a un delito conexo, pues, no tenemos que contemplar sólo el supuesto de un proceso independiente.

La LECRIM en la regulación de las medidas tecnológicas, contempla en su art. 588 bis i) la posibilidad de utilización de esos descubrimientos casuales, si bien resulta necesario tener presente que para la incorporación de esos descubrimientos o hallazgos a ese "otro proceso" se debe, en todo caso, respetar los principios del art. 588 bis a) de la LECRIM – excepcionalidad, necesidad, proporcionalidad, etc., de la medida–. Este control que debe ejercerse en este "otro proceso relacionado de manera directa" obedece al filtro de comprobación de legitimación de la injerencia en los derechos fundamentales – en este caso, en el art. 18 CE–[60].

Por tanto, podemos afirmar que los datos personales obtenidos en el marco de una OEI – emitida por España– podrán ser utilizados en otro proceso, siendo necesario en ese segundo proceso que la propia autoridad judicial realice un control sobre la sujeción a los principios del art. 588 bis a) LECRIM, a pesar que el art. 193 LRMRP no hace mención a ello.

Una cosa es la utilización de esos datos en otra causa penal, como excepción al principio de especialidad –como se establece en el apdo. 2 del art. 4 de la Directiva 2016/680/UE– y, otra muy diferente, es abrir la puerta a la limitación de derechos bajo la premisa de la amenaza grave e inminente para la seguridad pública, pues nos movemos, una vez más, entre el derecho de protección de datos personales y en la protección de la seguridad pública.

C.- Otra cuestión que surge es la posibilidad de utilizar los datos recabados en el marco de una investigación penal –a través de una OEI– "con otros fines", debiendo recabarse el consentimiento de la autoridad del Estado de ejecución o del titular de los datos. Significa ello, que ¿podríamos utilizar los datos para un proceso administrativo, por ejemplo?. La imprecisión del legislador puede generar dudas a futuro, pues, la frase "otros fines" puede dar cabida a multitud de situaciones en las que pueda utilizarse los datos personales obtenidos amparados en el precepto. Y además, contempla la posibilidad que el titular de los datos consienta para darle otra utilidad a esos datos, sin legitimación para valorar si concurre los supuestos de necesidad y proporcionalidad, resulta, a todas luces, incoherente con el principio de especialidad.

Si nos remitimos a la Directiva 2016/680/UE, el art. 4.2 habilita la utilización de los datos personales para otro fin distinto de aquél para el que se recogieron los datos personales, permitiéndose el tratamiento por *el mismo responsable o por otro para los fines establecidos en el apdo.1 del art.1.* De la lectura del apdo.1 del art. 1 de la Directiva 2016/680/UE podemos afirmar que los fines para los que pueden utilizarse los datos obtenidos son la prevención, investigación, detección o enjuiciamiento, por tanto, no se contempla el uso de esos datos en un proceso administrativo.

A mayor abundamiento, y en clara referencia a los procedimientos en los que puede emitirse una OEI –art.186.2 de la LRMRP y 4 de la DOEI– podrán ser objeto en procedimientos administrativos que puedan dar lugar a un procedimiento penal, supuesto que no es posible en el caso de España, por tanto, esto viene a reforzar la respuesta a la pregunta formulada *ut supra,* no siendo posible utilizar los datos obtenidos en un procedimiento administrativo.

60. GONZÁLEZ CANO, María Isabel, «Garantías del investigado y acusado en orden a la obtención, cesión y tratamiento de datos personales en el proceso penal. A propósito de la Directiva (UE) 2016/680 y su impacto en materia de prueba penal» en VVAA (Dir. GONZÁLEZ CANO, María Isabel) *Orden Europea de Investigación y prueba transfronteriza en la Unión Europea,* Tirant lo Blanch, Valencia, 2019, págs. 99 y ss (en prensa).

IV.- REFLEXIÓN FINAL

La era digital ha supuesto un flujo de datos personales que muchas veces el propio titular de los mismos desconoce el tratamiento que se le va a dar a sus datos personales.

Antes de la entrada en vigor del RGPD, en determinadas ocasiones se vulneraba la legislación por parte de las entidades que almacenaban los datos. Actualmente, parece que se abren nuevos horizontes para el derecho a la protección de datos de carácter personal. Con la entrada en vigor del RGPD se han reforzado los derechos del interesado, ampliándose el elenco de derechos, en aras de fortalecer el control por parte del interesados de sus datos personales.

En el ámbito de la prevención, investigación y enjuiciamiento, en cuanto a la protección de los datos personales, se ha avanzado significativamente, respecto al instrumento predecesor DM 2008/977/JAI, con la promulgación de la Directiva 2016/680/UE. Consideramos necesario que la mencionada Directiva sea objeto de implementación en el ordenamiento jurídico español, pues si bien es cierto que el investigado y/o acusado tiene reconocidos sus derechos procesales, entendemos que los derechos contemplados en la Directiva 2016/680/UE operan de forma complementaria a los derechos y garantías procesales, pues no estaría de más que en el marco del proceso penal el investigado y/o acusado conozca los derechos que le amparan con respecto a sus datos personales, como son la posibilidad de rectificarlos, suprimirlos, plantear una reclamación ante la autoridad de control, etc.

Por otro lado, incidencia directa con el intercambio de datos y la salvaguarda del derecho de protección de datos personales va a tener la DOEI –y la LRMRP–. En referencia a la transposición que hace el legislador español, se suscitan dudas respecto al fin que que puedan darse a los datos obtenidos a través de la ejecución de una OEI en otro Estado miembro diferente al Estado español. Por un lado, el legislador español contempla la posibilidad que los datos recabados en el Estado de ejecución –diferente al español– puedan utilizarse de manera directa en otro proceso o, bien, para prevenir una amenaza grave e inminente para la seguridad pública. En ambos casos, suponen una excepción al principio de especialidad, excepciones que no habrán de aplicarse sin control alguno. En el supuesto que los datos se utilicen en un proceso distinto, nos movemos en el campo del hallazgo casual, supuesto que no impide que en el marco de una investigación de un delito concreto se obvie aquellos indicios de delito que se presentan casualmente y que son diferentes a la investigación objeto de la medida adoptada. En particular, en referencia a los datos obtenidos en el Estado de ejecución, entendemos que podrían utilizarse en otro proceso distinto siempre que se cumpla, para su incorporación, el doble control de legitimidad –esto es, con sujeción a los principios rectores del art. 588 bis a). En la otra excepción prevista, para el caso de amenaza grave e inminente –por ejemplo, casos de terrorismo– la Directiva 2016/680/UE, prevé la transmisión de datos personales a otros Estados miembros o terceros países sin sometimiento a autorización previa. Si bien, en el presente supuesto resulta llamativo el hecho que se puedan limitar los derechos de investigados y/o acusados–acceso, información, supresión, rectificación–, sin que la misma contemple un cauce para controlar la proporcionalidad, pues se puede hacer una limitación *sine die.*

Además, el art. 193.1 establece la posibilidad de utilización de estos datos "con otros fines". Al respecto, debemos afirmar que ni la Directiva 2016/680/UE ni el propio art. 186.2 de la LRMRP contemplan la posibilidad de utilizar esos datos en un procedimiento distinto del penal, esto es, por ejemplo, en un procedimiento administrativo.

Ahora bien, amparados en la prevención y persecución de delitos, ¿significa esto que los ciudadanos estamos cediendo nuestros derechos fundamentales a favor de la seguridad nacional?. Aquí se plantea el difícil equilibrio entre la seguridad y los derechos fundamentales, cuestión que no tiene una fácil

respuesta, si bien debe buscarse una ponderación adecuada[61]. Fundamental va a resultar el principio de disponibilidad en el marco de la cooperación judicial penal a efectos represivos, pero el intercambio de datos personales no debe amparar cualquier actuación que se extralimite del principio de especialidad, de lo contrario, los datos personales estarán a merced de cualquier investigación genérica de delitos.

61. Resumen del Dictamen del SEPD, de 7 de marzo de 2012 sobre el paquete legislativo de reforma de la protec- ción de datos, DOUE C 192, de 30 de junio de 2012. Subraya el SEPD que *"todo desvío de las normas genera- les de protección de datos debería quedar debidamente justificado por una ponderación equilibrada entre el interés público de aplicación de las leyes y los derechos fundamentales de los ciudadanos"*.

BIBLIOGRAFÍA

- APARICIO SALOM, Javier, «Derechos del interesado (Arts. 12-19 RGPD. Arts.11-16 LOPDGDD)» en VVAA (coord. LÓPEZ CALVO, José) *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019.
- DE HOYOS SANCHO, Montserrat, «Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos», en VVAA (Dir. ARANGÜENA FANEGO, Coral) *Espacio europeo de libertad, seguridad y justicia: últimos avances en cooperación judicial penal,* Lex Nova, Valladolid, 2010.
- GALÁN MUÑOZ, Alfonso, «La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea» en AAVV (Dir. COLOMER HERNÁNDEZ, Ignacio) *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea",* Aranzadi, Cizur Menor, 2015.
- GALÁN MUÑOZ, Alfonso, «Los nuevos instrumentos de prevención y lucha contra el nuevo terrorismo: malas noticias para la intimidad y otros derechos fundamentales» en VVAA (Dir. COLOMER HERNÁNDEZ, Ignacio) *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios,* Aranzadi, Cizur Menor, 2017.
- GÓMEZ COLOMER, Juan Luis y PLANCHADELL GARGALLO, Andrea, «Prueba prohibida», VVAA (dir. por GONZÁLEZ CANO, María Isabel), *La prueba. Tomo II. La prueba en el proceso penal,* Tirant lo Blanch, Valencia, 2017.
- GONZÁLEZ CANO, María Isabel, «Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial penal en la Unión Europea», en VVAA (Dir. COLOMER HERNÁNDEZ, Ignacio) *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios,* Aranzadi, Cizur Menor, 2017.
  - «Garantías del investigado y acusado en orden a la obtención, cesión y tratamiento de datos personales en el proceso penal. A propósito de la Directiva (UE) 2016/680 y su impacto en materia de prueba penal» en VVAA (Dir. GONZÁLEZ CANO, María Isabel) *Orden Europea de Investigación y prueba transfronteriza en la Unión Europea,* Tirant lo Blanch, Valencia, 2019, págs. 99 y ss (en prensa).
  - «Reflexiones sobre libre circulación de datos personales y principio de disponibilidad en el ámbito de la cooperación judicial penal en la Unión Europea» en VVAA (coord. CACHÓN CARDENAS, Manuel y FRANCO ARIAS, Just) *Derecho y Proceso. Liber Amicorum del Profesor Francisco Ramos Méndez,* Atelier, Barcelona, 2018, Vol. II, págs. 1073 y ss.
- GUTIÉRREZ ZARZA, Ángeles, «La protección de las personas físicas en lo que respecta a su derecho a la intimidad y los datos personales por las autoridades de emisión y ejecución de las órdenes europeas de investigación» en VVAA (Dir. ARANGÜENA FANEGO, Coral y DE HOYOS SANCHO, Montserrat) *Garantías procesales de investigados y acusados. Situación actual en el ámbito de la Unión Europea,* Tirant lo Blanch, Valencia, 2017.
- MARTÍNEZ PÉREZ, Fernando y POZA CISNEROS, María, «El principio de disponibilidad: antecedentes penales y convenio de Prüm» en VVAA (Dir. CARMONA RUANO, Miguel, GONZÁLEZ VEGA, Ignacio. U, MORENO CATENA, Víctor) *Cooperación Judicial Penal en Europa,* Madrid, Dykinson, 2013.
- MUÑOZ RODRÍGUEZ, Joaquín, «Disposiciones generales. Título I (Arts. 1-5 RGPD. Arts. 1-3 LOPDGDD)» en VVAA (coord. LÓPEZ CALVO, José) *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019.
- PILLADO GONZÁLEZ, Esther, «Difícil equilibrio entre seguridad y salvaguarda del derecho a la protección de datos personales en la prevención, investigación y represión de delitos en la Unión Europea» en VVAA (Dir. GONZÁLEZ CANO, María Isabel) *Integración europea y justicia penal,* Tirant lo Blanch, Valencia, 2018.

- PLAZA PENADÉS, Javier, «El nuevo marco normativo de la protección de datos», en *Diario La Ley,* Sección Actualidad Civil, nº 5, mayo de 2018, Editorial Wolters Kluwer.
- PUYOL MONTERO, Javier, «Transparencia de la información y derecho de acceso de los interesados» en VVAA (Dir. RALLO LOMBARTE, Artemi) *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Tirant lo Blanch, Valencia, 2019.

ÁPENDICE NORMATIVO

- Convenio nº 185, del Consejo de Europa, de 23 de noviembre de 2001, sobre Ciberdelincuencia. BOE 17 de septiembre de 2010.
- Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. DOUE L 210, de 6 de agosto de 2008.
- Decisión Marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea. DOUE L 386, de 29 de diciembre de 2006.
- Decisión Marco 2008/977/JAI, protección de datos personales tratados en el contexto de la cooperación policial y judicial en materia penal. DOUE L 350/60, de 30 de diciembre de 2008.
- Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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. DOUE L 281, de 23 de noviembre de 1995.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. DOUE L201/37, de 31 de julio de 2002.
- Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 , sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. DOUE L105/54, de 13 de abril de 2006.
- Directiva 2014/41 (UE) del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal. DOUE 130, de 1 de mayo de 2014.
- Directiva (UE) 2016/680, de 27 de abril de 2016, del Parlamento Europeo y del Consejo, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y sobre la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. DOUE L 119/89, de 4 de mayo de 2016.
- Directiva 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. DOUE L119, de 4 de mayo de 2016.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. BOE núm. 251, de 19 de octubre de 2007.
- Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea. BOE núm. 282, de 21 de noviembre de 2014.
- Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. BOE núm. 242, de 9 de octubre de 2007.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 6 de diciembre de 2018.

- Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. DOUE L008, de 12 de enero de 2001.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ CE. DOUE L 119/88, de 4 de mayo de 2016.

JURISPRUDENCIA

- TJUE, Gran Sala, Sentencia de 8 de abril de 2014, asuntos C-293/12 y C−594/12 (Digital Rights Ireland Ltd; Kärntner Landesregierung)
- TJUE, Gran Sala, Sentencia de 21 de diciembre de 2016, asunto C203/15 y 698/15 (Tele2 Sverige AB y Post- och telestyrelsen; Secretary of State for the Home Department y Tom Watson y otros).
- TJUE, Gran Sala, Sentencia de 2 de octubre de 2018, asunto C-207/16 (AP Tarragona).