LA NUEVA NORMATIVA EUROPEA PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

THE NEW EUROPEAN REGULATIONS ON PERSONAL DATA PROTECTION

ENRIQUE PÉREZ-LUÑO ROBLEDO
Universidad de Sevilla

Fecha de recepción: 4-7-18
Fecha de aceptación: 9-10-18

Resumen: *El 27 de abril de 2016, la UE promulgó tres importantes textos normativos que constituyen ahora el marco de tutela de los datos personales de los ciudadanos europeos. Se trata del Reglamento General de protección de datos personales, que sustituye a la Directiva 95/46; de la Directiva para la protección de los datos personales en materia de infracciones y sanciones penales y de la Directiva sobre los datos PNR (Passenger Name Record). En este trabajo se analizan los principales aspectos de estas innovaciones normativas dirigidas a la tutela de los datos personales en el ámbito de la UE. Se analizan, asimismo, las principales garantías de los ciudadanos europeos para el acceso y control de las informaciones que les afectan, reguladas en la nueva normativa de la UE.*

Abstract: *On April 27, 2016, the EU enacted three significant legal texts which now provide the legal framework for the personal data protection of the EU citizens. This is about The General Data Protection Regulation (GDPR) that replaces the EU Directive 95/46; The Directive (EU) 2016/680 on the protection of natural persons with regards 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 the Directive (EU) 2016/681 on Passenger Name Record (PNR).*
This paper will analyse the key aspects of these regulatory innovations aimed at protecting the personal data at the EU level.
Similarly, it will be analysed the main guarantees for the EU citizens in order to the access and control of information that affect them addressed by the new Community legislation.

ISSN: 1133-0937
DOI: 10.14679/1115

Palabras clave: datos personales, derecho a la intimidad, habeas data, derechos ARCO, derecho al olvido, derechos fundamentales, derechos de oposición, Nuevas Tecnologías (NT), Tecnologías de la Información y de la Comunicación (TIC)

Keywords: personal data, right to privacy, *habeas data*, ARCO rights (access, rectification, cancellation and objection), right to be forgotten, fundamental rights, right of opposition, emerging technologies, latest technologies, new technologies, Information and Communication Technologies (ICT)

1. PLANTEAMIENTO

En la Unión Europea (UE), desde los inicios del desarrollo tecnológico, se suscitó el interés por conjugar el aprovechamiento económico de esos avances con la protección de los derechos fundamentales de los ciudadanos miembros de la UE[1]. Esa sensibilidad por la protección de los datos personales frente a abusos informáticos tuvo como modelo, la acción tutelar del Consejo de Europa. El proceso de garantía de los datos personales en la UE, no se ha caracterizado por su progresión lineal, sino por sus continuos avances y retrocesos[2].

En el marco del Derecho de la UE, tradicionalmente ha prevalecido la protección del componente económico del intercambio de datos de carácter personal, pero sin que ello haya significado un descuido de ciertas garantías de seguridad surgidas a raíz de la creación de un espacio común sin fronteras. Progresivamente la evolución del sistema jurídico europeo se ha traducido en la promulgación de la Directiva 95/46 UE específica para la protección de datos personales y la proclamación en el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea del derecho a la protección de datos de carácter personal, derecho que posteriormente se incluirá en dos preceptos del Tratado por el que se instituye una Constitución para Europa[3], incluyén-

[1] A. SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática en la Unión Europea,* con Prólogo de A. E. Pérez Luño, Publicaciones de la Universidad de Sevilla, Sevilla, 1998; Idem, *Internet y la sociedad europea de la información: implicaciones para los ciudadanos*, con "Prólogo" de A.E. Pérez Luño, Publicaciones de la Universidad de Sevilla, 2001, pp.26 ss.

[2] Cfr., A. GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2ª ed., 2009, passim.; M.C. GUERRERO PICÓ, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson & Civitas, Madrid, 2006, pp. 55 ss.

[3] Cfr., M. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006, pp. 227 ss.

dose también en el Tratado de Lisboa de 2009 y convirtiéndose, por tanto, en derecho vigente de UE.

El 27 de abril de 2016 el Parlamento y el Consejo de la UE aprobaron tres textos normativos básicos para la protección y el tratamiento de los datos personales en el seno de la UE. Se trata del Reglamento 2016/679 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 (Reglamento General de protección de datos) y por el que se deroga la Directiva 95/46/CE; la Directiva 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo; y la Directiva 2016/681 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.

2. ENTRADA EN VIGOR Y CARACTERES GENERALES DE LA NUEVA NORMATIVA

El primer aspecto que merece atención es el referente a la aplicación del Reglamento. En efecto, tal como prescribe su artículo 94, la derogación de la Directiva 95/46 tendrá efecto a partir del 25 de mayo de 2018. No obstante, el art. 99 del Reglamento establece que su vigencia comenzará a partir de los 20 días de su publicación en el Diario Oficial de la Unión Europea, que tuvo lugar el pasado 4 de mayo de 2016, aunque en dicho artículo se reitera lo previsto en el mencionado art. 94 sobre su aplicación y plenos efectos a partir de la fecha de 25 de mayo de 2018.

Por lo que respecta a la Directiva 2016/ 680, conviene reseñar que su art. 63 prescribe que los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en ella. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones y las aplicarán a partir del 6 de mayo de 2018[4].

[4] Sobre la futura transposición de esta Directiva a nuestro ordenamiento jurídico vid. I. COLOMER HERNÁNDEZ, "A Propósito de la compleja trasposición de la Directiva 2016/680 relativa al tratamiento de datos personales para fines penales", *Diario La Ley*, núm. 9179, 2018.

Tras más de veinte años de vigencia de la Directiva 95/46, en el que ha cumplido una función relevante para la tutela de los datos personales en el ámbito europeo, se ha culminado ahora el proceso de su necesaria renovación para adaptar la normativa de la UE a las nuevas exigencias y requerimientos de nuestro tiempo.

Para cumplir con ese reto con fecha de 17 de diciembre de 2015 el Comité de Libertades Civiles del Consejo y del Parlamento de la UE, aprobó con 48 votos a favor, 4 votos en contra y 4 abstenciones, una redacción definitiva de los textos del Reglamento y las Directivas de protección de datos. En dicha redacción los aspectos más innovadores respecto a los Proyectos aquí estudiados son los que hacen referencia a un reforzamiento de la posición de los particulares frente a los datos personales almacenados por sociedades multinacionales, con inclusión expresa de su oposición a que esos datos puedan ser utilizados o transmitidos al margen de los supuestos que han autorizado la inclusión en sus ficheros, así como el reconocimiento expreso del derecho al olvido.

Representa un rasgo novedoso de la nueva normativa su propósito de garantizar que el responsable del tratamiento de datos personales responda de la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema de información para resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. Con todo ello, se refuerzan también las garantías de los titulares de los datos personales frente a nuevas formas de agresión a los equipos informáticos que pudieran redundar en una vulneración de los datos que les conciernen.

3. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El Reglamento ahora aprobado, trata de arbitrar fórmulas para facilitar al interesado el ejercicio de sus derechos, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los

datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar instrumentos para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos[5].

Se obliga al responsable del tratamiento a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas.

El derecho de acceso, también denominado *habeas data*[6], se configura en el Reglamento, como un derecho de los interesados a acceder a los datos personales recogidos que le conciernan y a ejercer la acción procesal tutelar de ese derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas[7]. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales[8].

Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y,

---

[5] Cfr.: A. GARRIGA DOMÍNGUEZ, "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", *Derechos y Libertades,* núm. 38, 2018, pp. 107 ss. Vid., también: B. ADSUARA VARELA, "El ciudadano frente al Reglamento", en el vol. col., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* Wolters Kluwer, Madrid, 2018, pp. 163 ss.; J. APARICIO, "Derecho de oposición y decisiones individuales automatizadas. Limitaciones", en ibidem, pp. 409 ss.

[6] E. PÉREZ-LUÑO ROBLEDO, *El procedimiento de habeas data. El derecho procesal ante las nuevas tecnologías*, Dykinson, Madrid, 2017, *passim*.

[7] J. M. PÉREZ GÓMEZ, "Especialidades en el sector sanitario", en el vol. col., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* cit., pp. 195 ss.

[8] Cfr.: A. GARRIGA DOMÍNGUEZ, "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", cit., pp.129 ss.

en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud.

Conviene recordar como un antecedente de la actual normativa reglamentaria de la UE, una importante sentencia sobre el derecho de acceso. Se trata del caso Haralambie contra Rumania[9]. En este supuesto el Tribunal de Estrasburgo establece y desarrolla lo que podría considerarse como núcleo básico del *habeas data* europeo. En efecto, en esta decisión se plantea, y constituye su centro de gravedad, el derecho de acceso que correspondía al ciudadano rumano Haralambie a los archivos policiales, en los que constaban informaciones personales que afectaban a su vida privada y habían sido recabados durante la etapa del régimen comunista. Tras la instauración del Estado de Derecho las autoridades policiales no sólo no destruyeron esos datos, sino que dificultaron su acceso al ciudadano concernido.

El TEDH, a partir del artículo 8 de la Convención y del Convenio 108, consideró que toda persona tiene derecho a acceder a los datos personales que le conciernen y a solicitar la rectificación de los erróneos, y en su caso, a la cancelación de aquellos que hubieran sido indebidamente registrados o hubiera pasado el tiempo que legitimaba su tratamiento. El TEDH reconoce así el *derecho al olvido* de aquellas informaciones que, aunque pudieron ser legalmente recabadas en un determinado momento, pasado el tiempo han perdido la razón que legitimaba su tratamiento. De este modo, ninguna persona puede ser "prisionera de su pasado", en particular, cuando esos datos pretéritos pueden condicionar su situación presente, sin causa, razonable que lo justifique.

En esta sentencia, además, los magistrados de Estrasburgo señalaron que las informaciones policiales sobre las que se deseaba ejercitar la acción de *habeas data*, habían sido elaboradas con fines de control ideológico, para amedrentar a la población y garantizar su actitud sumisa ante un sistema político totalitario. Todo lo cual condujo a una sentencia que reconocía plenamente el derecho de acceso invocado por el demandante.

[9] STEDH de 27 de octubre de 2009, Haralambie contra Rumania, Rec. n. 21737/03.

Al igual que en el diseño planteado en la Propuesta de Reglamento, en el texto definitivo, el *habeas data* aparece regulado en el art. 15, con ligeras variantes respecto a su redacción anterior. Se halla incluido en la Sección 2 (Información y acceso a los datos personales) del Capítulo III en el que se consagran los: "Derechos del interesado". La redacción definitiva de este artículo es la siguiente:

> "Derecho de acceso del interesado
> 1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:
>   a) los fines del tratamiento;
>   b) las categorías de datos personales de que se trate;
>   c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
>   d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
>   e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
>   f) el derecho a presentar una reclamación ante una autoridad de control;
>   g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
>   h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
> 2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.
4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros".

Los principales rasgos innovadores que se aprecian en la nueva redacción del artículo, se refieren, básicamente, a los siguientes aspectos. Se añade en el apartado c) del nuevo texto una referencia expresa a las "organizaciones internacionales" como destinatarias de la transferencia de datos.

En el apartado d) del texto definitivo se sustituye la exigencia de un plazo taxativo de conservación de los datos personales, por la mera posibilidad de establecer ese plazo, exponiendo los criterios para determinar dicho plazo.

En el apartado f), la Propuesta preveía el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma. En el Reglamento aprobado se suprime la necesidad de aportar los datos de contacto de la autoridad de control.

En el apartado h) se hace alusión expresa a que el responsable del tratamiento informe de la posibilidad de que los datos del interesado puedan utilizarse para la toma de decisiones automatizadas, incluida la elaboración de perfiles.

En el apartado 2 del mencionado art. 15 del Reglamento 2016/679, se incluye una cláusula de garantía muy importante que hace referencia a que cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46, en el que dichas garantías se especifican, relativas a la transferencia. Con ello, se refuerza el dominio de los titulares de datos personales sobre los mismos y se extiende la tutela de su *habeas data* al conocimiento de cualquier transferencia de sus datos a nivel internacional[10].

Esta garantía ha podido ser motivada en su redacción por la Sentencia del Tribunal de Justicia de la UE, de fecha 6 de octubre de 2015, referente al denominado caso "Europa vs Facebook".

[10] J. APARICIO, "Derechos del interesado", en el vol. col., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* cit., pp. 363 ss.

Los antecedentes de este supuesto parten de la denuncia del ciudadano europeo Max Schrems contra Facebook por vulnerar la reglamentación europea de protección de datos personales que fue presentada ante la Agencia de Protección de Datos de la República de Irlanda.

Motivó esta demanda el hecho de que Maximillian Schrems, ciudadano austriaco, era usuario de Facebook desde 2008. Como ocurre con los demás usuarios que residen en la UE, los datos proporcionados por Schrems a Facebook fueron transferidos total o parcialmente de la filial irlandesa de dicha red social a servidores situados en territorio de los Estados Unidos, donde fueron objeto de tratamiento. El demandante consideró que dicho tratamiento vulneraba la protección europea de sus datos personales.

Dicha Agencia la desestimó por entender en su Decisión de 26 de julio de 2000 que la Comisión Europea había considerado que, en el marco del régimen denominado de "puerto seguro", Estados Unidos garantiza un nivel adecuado de protección de los datos personales transferidos.

El demandante, tras la denegación de la Agencia, la reprodujo ante el Tribunal Supremo (High Court) Irlandes. Dicho Tribunal planteó, con fecha 17 de julio de 2014, una cuestión prejudicial ante el Tribunal de la UE relativa a la interpretación de la legislación europea al respecto.

En su Sentencia el Tribunal de Luxemburgo ha establecido que el artículo 25, de la Directiva 95/46 de protección de datos, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro de la UE, a la que se refiere el artículo 28 de esa Directiva, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

La principal consecuencia que dimana de la Sentencia aquí aludida, en cuanto se refiere a la tutela de la protección de datos, en relación con su transferencias a terceros países, es que reconoce un derecho de los ciudada-

nos europeos para acceder y controlar sus datos personales incluidos en los ficheros de empresas que operan en Europa, aunque sus sedes radiquen en territorio extra europeo.

Estas garantías han sido básicamente asumidas en el texto definitivo del Reglamento, en el seno del precitado apartado 2 del artículo 15.

Un aspecto novedoso de la redacción del Reglamento, antes no incluido en la Propuesta, consiste en la posibilidad de que el responsable pueda percibir a partir de la segunda copia de los datos personales objeto de tratamiento facilitados a los interesados, un canon razonable basado en los costes administrativos de dichas copias. Con ello se pretende evitar la petición abusiva de copias por parte de los titulares. Estos tienen derecho a la información, pero no a que se les suministren cuantas copias deseen, a costa del responsable del tratamiento.

Una importante limitación incluida en el Reglamento se refiere a que el derecho a obtener la copia de los datos personales objeto de tratamiento por parte de los interesados, no afectará negativamente a los derechos y libertades de otros.

El Reglamento inscribe el *habeas data* en el marco de los derechos ARCO, estableciendo una regulación sistemática y armonizada de estos derechos y de su ejercicio ante los nuevos desarrollos tecnológicos, en especial, ante la enorme difusión de las redes sociales. Así, basándose en el artículo 12, letra b), de la Directiva 95/46, el artículo 16 establece el derecho del interesado a la rectificación.

El artículo 17 establece el derecho del interesado al olvido y de supresión. Asimismo elabora y especifica el derecho de supresión que se establece en el artículo 12, letra b), de la Directiva 95/46 y establece las condiciones del derecho al olvido, incluida la obligación del responsable del tratamiento que haya difundido los datos personales de informar a los terceros sobre la solicitud del interesado de suprimir todos los enlaces a los datos personales, copias o réplicas de los mismos. También integra el derecho a que se restrinja el tratamiento en determinados casos, evitando la ambigüedad del término "bloqueo"[11].

La actualidad y repercusión mediática del denominado "caso Google", Sentencia del 13 de mayo de 2014 del Tribunal de Justicia de la UE, ha moti-

[11] Cfr. J. APARICIO, "Derechos del interesado", en el vol. col., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* cit., pp. 393 ss.

vado un especial interés del legislador europeo en la regulación del "derecho al olvido", que ha hallado puntual acogida en el nuevo Reglamento.

Dicha sentencia tuvo origen en la reclamación que el Sr. Costeja González presentó contra La Vanguardia Ediciones y frente a Google Spain y Google Inc. (en adelante "Google"), ante la Agencia Española de Protección de Datos (AEPD). Su reclamación se basaba en que, cuando un internauta introducía su nombre en el motor de búsqueda de Google, obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia del año 1998, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social.

Dicha reclamación fue desestimada por la AEPD en lo que afectaba a La Vanguardia y en cambio fue estimada en relación con Google. Esta empresa americana interpuso dos recursos ante la Audiencia Nacional que, tras acumularlos, decidió suspender el procedimiento y plantear al Tribunal de Justicia de la UE unas cuestiones prejudiciales sobre la aplicabilidad del Derecho Comunitario a este supuesto.

En relación con dichas cuestiones, la sentencia del tribunal de la UE estableció que la actividad llevada a cabo por los motores de búsqueda debe calificarse como "tratamiento de datos personales" cuando la información a la que acceden contenga datos personales. De conformidad con la legislación europea (Directiva 95/46), la actividad de un motor de búsqueda consistente en hallar información publicada o puesta en internet por terceros, indexada de manera automática, almacenada temporalmente y puesta a disposición de los internautas según un orden de preferencia determinado debe calificarse como "tratamiento de datos", y dicho motor deberá ser considerado "responsable del tratamiento".

El Tribunal de Luxemburgo consideró que, siempre que concurran ciertos requisitos y previa solicitud del interesado, el responsable de un motor de búsqueda está obligado a eliminar de la lista de datos obtenida, tras una búsqueda efectuada a partir del nombre de la persona concernida, todos los datos personales de dicha persona, vinculados a páginas web publicadas por terceros y que contienen información relativa a esa persona, incluso en el supuesto de que esos datos no se borren previa o simultáneamente de esas páginas web y aún cuando la publicación en dichas páginas sea en sí misma lícita.

El Tribunal Europeo consideró que la persona concernida tiene derecho a que la información que le afecta y publicada legalmente por terceros no

se ponga a disposición del público en general mediante su inclusión en una lista de resultados, debido a que esos datos o información pueden perjudicarle o que, simplemente, el interesado desee que esos datos e información se olviden tras un determinado lapso de tiempo. Un supuesto distinto es que, por razones concretas (tales como la naturaleza de los datos publicados o la condición de la persona afectada), la injerencia en el derecho del afectado esté justificada por el interés preponderante del público a conocer y tener acceso a esa información. Por ello, Google tras la sentencia del Tribunal de Luxemburgo, se ha apresurado a habilitar un procedimiento para que los interesados puedan ejercitar su derecho de oposición, pero justifican las excepciones a acceder a dicho derecho en función de fines de interés público o social. Entre los ejemplos puestos por la empresa californiana, se alude a la denegación cuando se trate de datos relativos a estafas financieras, negligencia profesional, condenas penales o corrupción de funcionarios públicos… Con estos ejemplos la empresa norteamericana justifica las restricciones ante determinadas demandas, en función a situaciones que producen alarma social y que, por tanto, la opinión pública rechaza el "olvido" de esos comportamientos.

La importancia de esta sentencia para la garantía del *habeas data* europeo, estriba en su contribución a la tutela del derecho de oposición y, por tanto, de un derecho "al olvido", en el seno de todos los Estados que forman parte de la UE. Como se tuvo ocasión de exponer en las páginas dedicadas a la delimitación conceptual del *Habeas data*, esta categoría, en su acepción amplia no se limita al reconocimiento del derecho al acceso, sino que se extiende a los denominados derechos "ARCO" (Acceso, Rectificación, Cancelación, Oposición), por ello, toda la temática relativa al derecho de oposición y, consiguientemente, al denominado derecho al "olvido", se inscribe de pleno en el ámbito teórico y en la incidencia práctica del *habeas data.*

No huelga tampoco recalcar, que esta sentencia especifica quien tiene la responsabilidad y la obligación, de retirar la información o los enlaces a informaciones que puedan ser lesivas para las personas y que, además, carezcan de relevancia informativa.

El Tribunal de la UE se planteó, también, si el derecho del perjudicado llega al punto de generar la obligación de retirar la información publicada en la fuente o si aquel derecho alcanza solamente a la obligación del motor de búsqueda de no posibilitar enlaces a aquellas fuentes o noticias que perjudiquen el derecho del recurrente, aun cuando dicha información sea totalmen-

te lícita. En este aspecto, la sentencia opta por la segunda interpretación. Por ello, la sentencia obliga al motor de búsqueda a "ocultar" siempre que concurran ciertas circunstancias y previa solicitud del interesado, no poniendo a disposición del resto de internautas aquella información que contenga datos personales. En principio, dicha obligación no será extensible al responsable de la fuente de información publicada, pues éste, si los datos publicados son veraces y lícitos, se halla amparado por el derecho de libertad de expresión e información. Con ello, el Tribunal de Luxemburgo coincide con la resolución de la AEPD, que como se ha indicado *supra* sancionó a Google, pero no a La Vanguardia.

Inspirándose en esta sentencia, el Reglamento establece que los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un "derecho al olvido" si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento.

Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

Para una mayor garantía jurídica del "derecho al olvido" en el entorno *on-line*, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén elaborando tales datos

personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

El artículo 20 introduce el derecho del interesado a la portabilidad de los datos, es decir, a transferir datos de un sistema de tratamiento electrónico a otro, sin que se lo impida el responsable del tratamiento. A modo de condición previa y con el fin de seguir mejorando el acceso de las personas físicas a sus datos personales, establece el derecho de obtener del responsable esos datos en un formato electrónico estructurado y de uso habitual.

El artículo 21 establece el derecho de oposición del interesado. Se basa en el artículo 14 de la Directiva 95/46, con algunas modificaciones, especialmente por lo que respecta a la carga de la prueba y su aplicación en el marketing directo.

El artículo 22 se refiere al derecho del interesado a no ser objeto de una medida basada en la elaboración de perfiles, a los que ya se ha aludido *supra*. Con modificaciones y salvaguardias adicionales, se basa en el artículo 15, apartado 1, de la Directiva 95/46 en materia de decisiones individuales automatizadas, y toma en consideración la Recomendación del Consejo de Europa sobre la elaboración de perfiles[12].

Como es norma habitual en el Derecho comparado de protección de datos, el ejercicio de los derechos ARCO, no se halla exento de algunos límites y restricciones. La legitimidad de estas limitaciones, debe establecerse de manera clara e inequívoca, para evitar que la remisión a ellas pudiera servir de *alibi* para prácticas restrictivas injustificadas de la libertad informática o para vaciarla de contenido.

El artículo 23 aclara la facultad otorgada a la Unión o a los Estados miembros de mantener o introducir restricciones a los principios establecidos en los derechos de los interesados previstos en los artículos 12 a 22. Esta disposición se basa en el artículo 13 de la Directiva 95/46 y en las obligaciones que emanan de la Carta de Niza y el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, interpretados por el Tribunal de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos[13].

[12] Vid., Recomendación del Consejo de Europa CM/Rec (2010) 13.

[13] J. APARICIO, "Derecho de oposición y decisiones individuales automatizadas. Limitaciones", en el vol. col., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* cit., pp. 409 ss.

En la medida en que en una sociedad democrática sea necesario y proporcionado para salvaguardar la seguridad pública, incluida la protección de la vida humana especialmente en respuesta a catástrofes naturales u ocasionadas por el hombre, la prevención, investigación, y el enjuiciamiento de infracciones penales o de violaciones de normas deontológicas en las profesiones reguladas, otros intereses públicos de la Unión o de un Estado miembro, especialmente un importante interés económico o financiero de la Unión o de un Estado miembro, o la protección del interesado o de los derechos y libertades de otros, el Derecho de la Unión o la legislación de los Estados miembros pueden imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación y supresión o al derecho a la portabilidad de los datos, al derecho a oponerse, a las medidas basadas en la elaboración de perfiles, así como a la comunicación de una violación de datos personales a un interesado y a determinadas obligaciones afines de los responsables del tratamiento.

Inspirado en el artículo 28, apartado 4, de la Directiva 95/46/CE, el artículo 77 del Reglamento, establece el derecho de cualquier interesado a presentar una reclamación ante una autoridad de control. Asimismo especifica los organismos, organizaciones o asociaciones que pueden presentar una reclamación en nombre del interesado o, en caso de violación de los datos personales, con independencia de la reclamación de un interesado.

El artículo 78 se refiere al derecho de recurso judicial contra una autoridad de control. Se basa en la disposición general del artículo 28, apartado 3, de la Directiva 95/46/CE. Establece específicamente un recurso judicial por el que se obliga a la autoridad de control a actuar a raíz de una reclamación y aclara la competencia de los órganos jurisdiccionales del Estado miembro en que esté establecida la autoridad de control. Asimismo ofrece la posibilidad de que la autoridad de control del Estado miembro en el que resida el interesado, ejercite, en nombre del interesado, una acción ante los órganos jurisdiccionales de otro Estado miembro en el que esté establecida la autoridad de control competente.

Desde el punto de vista procedimental, debe hacerse referencia a los artículos 79, 80 y 81 del nuevo Reglamento que establece normas comunes para los procedimientos judiciales, incluidos los derechos de los organismos, organizaciones o asociaciones de representar a los interesados ante los tribunales, el derecho de las autoridades de control a ejercitar acciones legales y de los órganos jurisdiccionales a ser informados sobre los procedimientos para-

lelos en otro Estado miembro, y pudiendo suspender en tal caso el procedimiento[14]. Los Estados miembros están obligados a garantizar la celeridad de las actuaciones judiciales[15].

El artículo 82 establece el derecho a indemnización y responsabilidad. Se basa en el artículo 23 de la Directiva 95/46/UE, amplía este derecho a los daños y perjuicios causados por los encargados del tratamiento y aclara la responsabilidad de los corresponsables y coencargados del tratamiento.

El artículo 85 obliga a los Estados miembros a adoptar exenciones y excepciones a las disposiciones específicas del Reglamento cuando resulte necesario para conciliar el derecho a la protección de los datos de carácter personal con el derecho a la libertad de expresión. Se basa en el artículo 9 de la Directiva 95/46/UE, tal como ha sido interpretado por el Tribunal de Justicia de la UE en la sentencia de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia.

El Reglamento obliga a los Estados miembros a establecer salvaguardias específicas para el tratamiento y acceso del público a documentos oficiales (artículo 86), así como las condiciones para categorías especiales de datos, entre ellos los referentes a datos laborales (artículo 88) y tratamiento del número nacional de identidad (artículo 87). Conviene tener presente al respecto la polémica suscitada en la doctrina y en la jurisprudencia sobre protección de datos, por toda la temática referida al "identificador único", es decir, a la posibilidad de utilizar con fines de control social los documentos de identidad[16].

Son también objeto de garantías especiales y excepciones en cuanto al régimen general de su tutela, el tratamiento de datos personales con fines históricos, estadísticos y de investigación científica (artículo 89). Asimismo

[14] Este texto se funda y trae causa del artículo 5, apartado 1, de la Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales, DO L 328 de 15.12.2009, p. 42, Y el artículo 13, apartado 1, del Reglamento citado anteriormente en este trabajo, (UE) n° 1/2003 del Consejo, de 16 de diciembre de 2002, relativo a la aplicación de las normas sobre competencia previstas en los artículos 81 y 82 del Tratado, DO L 1de 4.1.2003, p.1.

[15] En función del artículo 18, apartado 1, de la Directiva 2000/31/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior ("Directiva sobre el comercio electrónico"), DO L 178 de 17.7.2000, p. 1.

[16] Sobre esta cuestión vid. A.E. PEREZ LUÑO, *Derechos humanos, Estado de Derecho y Constitución,* Tecnos, Madrid, 10ª ed., 2010, pp. 378 ss.

se establecen normas específicas sobre protección de datos de las Iglesias y Asociaciones religiosas (artículo 91)[17].

Se ha realizado una exposición detallada de los artículos del Reglamento referidos a la garantía de la protección de datos, que conforman el marco normativo en el que dicha institución se engloba y debe ser interpretada, de conformidad con un método sistemático de interpretación. Por ello, estos artículos aquí reseñados, constituyen el ámbito normativo básico para la aplicación de las garantías para la tutela de la protección de datos personales en el seno de la UE.

4. LA DIRECTIVA 2016/680 DE PROTECCIÓN DE DATOS DE LAS PERSONAS FÍSICAS RELATIVA A INFRACCIONES Y SANCIONES PENALES

La Directiva 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, permite el establecimiento de un marco de protección de datos que garantiza un alto nivel de protección de los derechos de los individuos a la vez que se respeta la naturaleza específica del ámbito de cooperación policial y judicial en materia criminal.

Su finalidad principal se cifra en conseguir que los datos personales utilizados dentro del ámbito de cooperación policial y judicial en materia criminal, sean tratados de modo que se garantice un nivel adecuado de seguridad y confidencialidad, en particular impidiendo el acceso sin autorización a dichos datos o el uso no autorizado de los mismos y del equipo utilizado en el tratamiento, teniendo en cuenta el desarrollo técnico existente y la tecnología, los costes de ejecución con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

El derecho de acceso a los datos personales, se encuentra reconocido en esta Directiva en su Capítulo III, referente a los derechos del interesado. A

[17] Cfr. J. FERNÁNDEZ ACEVEDO, "Disposiciones relativas a situaciones específicas de tratamiento", en el vol. col., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* cit., pp. 671 ss.

diferencia de lo que se había planteado en la Propuesta de esta Directiva, en la que el derecho de acceso venia regulado en su art. 12, en el texto definitivo aparece en el art. 14, formulado en los siguientes términos:

> "Derecho de acceso del interesado a los datos personales
> Con sujeción a lo dispuesto en el artículo 15, los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en caso de que se confirme el tratamiento, acceso a dichos datos personales y la siguiente información:
> a) los fines y la base jurídica del tratamiento;
> b) las categorías de datos personales de que se trate;
> c) los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular los destinatarios establecidos en terceros países o las organizaciones internacionales;
> d) cuando sea posible, el plazo contemplado durante el cual se conservarán los datos personales o, de no ser posible, los criterios utilizados para determinar dicho plazo;
> e) la existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado, o la limitación de su tratamiento;
> f) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma;
> g) la comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen".

Las principales diferencias que se aprecian en el texto de la Directiva, con respecto a la redacción contenida en la Propuesta, versan sobre los siguientes aspectos:

1) En el texto definitivo al aludir al tratamiento, se añade la expresión "base jurídica".
2) Se añade en el apartado c) del nuevo texto una referencia expresa a las "organizaciones internacionales" como destinatarias de la transferencia de datos.
3) En el apartado d) del texto definitivo se sustituye la exigencia de un plazo taxativo de conservación de los datos personales, por la mera posibilidad de establecer ese plazo, exponiendo los criterios para determinar dicho plazo.

El nuevo marco regulatorio europeo establecido por esta Directiva pretende asegurar una protección de datos consistente y de alto nivel para mejorar la confianza mutua entre las autoridades policiales y judiciales de los diferentes Estados miembros de la UE, contribuyendo así a una mayor libertad de flujo de datos y una efectiva colaboración entre las autoridades policiales y judiciales[18].

El artículo l5 establece que los Estados miembros podrán adoptar medidas legislativas que restrinjan el derecho de acceso, si así lo exige la naturaleza específica del tratamiento de datos en los ámbitos policial y de la justicia penal, y sobre la información del interesado relativa a una restricción de acceso.

En el art. 16 se establecen los distintos supuestos y modalidades del ejercicio del derecho de rectificación o supresión de datos personales y limitación de su tratamiento. A su vez, en el art. 17 se prescribe que, cuando se restrinja el acceso directo, el interesado debe ser informado de la posibilidad de recurrir al acceso indirecto a través de la autoridad de control, que debe ejercer el derecho en su nombre y ha de informar al interesado del resultado de sus verificaciones.

Desde el punto de vista procesal posee también interés incuestionable cuanto dispone el artículo 18 en relación con la tutela del derecho de acceso, respecto con datos utilizados en procedimientos penales. En dicho texto se prescribe que los Estados miembros dispondrán que los derechos de información, acceso, rectificación, supresión y limitación del tratamiento reconocidos en la Directiva, se ejercerán de conformidad con las normas nacionales de enjuiciamiento cuando los datos personales figuren en una resolución judicial o en un registro tratado en el curso de investigaciones y procedimientos penales.

En este artículo se establece, por tanto, que cuando los datos personales se sometan a tratamiento en el transcurso de investigaciones y procedimientos penales, los derechos de información, acceso, rectificación, supresión y restricción del tratamiento pueden ejercerse de conformidad con las normas nacionales relativas a los procedimientos judiciales.

En el artículo 29 se establecen medidas tendentes a garantizar la seguridad de los datos. Entre ellas, tiene especial incidencia para el objeto de esta

[18] Cfr. M. B. SÁNCHEZ DOMINGO, "La protección de datos personales en el espacio de libertad, seguridad y justicia. Especial consideración a las transferencias de datos a terceros países y organizaciones internacionales según la directiva 2016/680", en *Revista de estudios europeos*, núm. 69, 2017, pp. 17 ss.

investigación, lo previsto en el artículo 29.2, cuando prevé que en lo referente al tratamiento automatizado de datos, cada Estado miembro dispondrá que el responsable o el encargado del tratamiento, a raíz de una evaluación de los riesgos, implementará medidas destinadas a:

Art.29.2.a) denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento de datos personales (control de acceso a los equipamientos);

Art.29.2.e) garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado de datos solo puedan tener acceso a los datos para los que han sido autorizados (control del acceso a los datos);

Por último, la Directiva al enumerar las funciones de las autoridades de control prescribe, en su artículo 46, la obligación de los Estados miembros de establecer las funciones de esas autoridades. De modo especial, se alude en dicho artículo a la necesidad de que se regule la admisión a trámite y la investigación de las reclamaciones y el fomento de la sensibilización de la opinión pública sobre riesgos, normas, garantías y derechos. Cuando se deniegue o restrinja el acceso directo, una función propia de las autoridades de control en el contexto de esta Directiva es el ejercicio del derecho de acceso por cuenta de los interesados y de verificación de la licitud del tratamiento de datos.

La Directiva pretende, que cuando los Estados miembros hayan adoptado medidas legislativas que restrinjan, total o parcialmente, el ejercicio del *habeas data,* el interesado tenga derecho a solicitar que la autoridad nacional de control competente verifique la licitud del tratamiento. El interesado debe ser informado de este derecho. Cuando el acceso sea ejercido por la autoridad de control a petición del interesado, este debe ser informado del curso de su solicitud, por la autoridad de control, como mínimo, de que se han llevado a cabo las verificaciones necesarias y del resultado en cuanto a la licitud del tratamiento en cuestión.

Reiterando cuanto se dispone en el Reglamento sobre el principio de tratamiento leal de los datos personales, la Directiva tiende a consagrar como garantía del interesado, que sea informado, entre otras cosas, de la existencia de la operación de tratamiento y sus fines, del plazo de conservación de los datos, de la existencia del derecho de acceso, rectificación o supresión y del derecho a presentar una reclamación. Cuando los datos se obtengan de los interesados, estos también deben ser informados de si están obligados a facilitarlos y de las consecuencias, en caso de que no lo hicieran.

No es ocioso reiterar que esta Directiva, al igual que el Reglamento, hallaron su fundamento en el artículo 16, apartado 2, del Tratado de Lisboa, que es una nueva base jurídica específica para la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos, y por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y de normas relativas a la libre circulación de estos datos.

En definitiva, esta nueva Directiva de la UE, se propone garantizar un nivel uniforme y elevado de protección a las personas físicas titulares de los datos. Al propio tiempo, desea conjugar esta finalidad garantista con el reforzamiento de la confianza mutua entre las autoridades policiales y judiciales de los distintos Estados miembros y facilitando la libre circulación de datos y la cooperación entre las autoridades policiales y judiciales[19].

5. LA DIRECTIVA 2016/681 SOBRE DATOS DEL REGISTRO DE NOMBRES DE LOS PASAJEROS (PNR)

En la misma fecha que el Reglamento y la Directiva ya analizados, la UE promulgó la Directiva 2016/681 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. Este texto normativo tiene su antecedente en el "Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano", que data del año 2010 y fue elaborado por el Consejo Europeo.

El objeto de esta nueva Directiva consiste entre otras cosas, en garantizar la seguridad, proteger la vida y la seguridad de los ciudadanos y crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes[20].

En este texto se establecen algunas garantías básicas en materia de protección de datos. Entre ella, reviste especial interés la que en el ámbito del

[19] Sobre la futura transposición de esta Directiva a nuestro ordenamiento jurídico vid. I. COLOMER HERNÁNDEZ, "A Propósito de la compleja trasposición de la Directiva 2016/680 relativa al tratamiento de datos personales para fines penales", cit.

[20] Para una valoración general de esta Directiva vid. M. A. CATALINA BENAVENTE, "La Directiva Europea (UE) 2016/681, de 27 de abril de 2016, relativa a la utilización de los datos por en la lucha contra el terrorismo y la delincuencia grave (1), *Diario La Ley*, núm. 8801, 2016.

tratamiento de los datos PNR, hace referencia a que los Estados miembros velarán para que el responsable de la protección de datos tenga acceso a todos los datos tratados por la UIP (unidad única de información sobre los pasajeros). Si el responsable de la protección de datos considera que el tratamiento de un dato cualquiera no ha sido lícito, podrá remitirlo a la autoridad nacional de control (art. 6.7).

La Directiva establece, en su art. 10.1, que Europol tendrá derecho a solicitar datos PNR o el resultado del procesamiento de dichos datos a las UIP de los Estados miembros dentro de los límites de sus competencias y para el desempeño de sus funciones.

Tiene especial relevancia, a efectos de la tutela de los datos personales, cuanto proclama el art. 12. En cuyo apartado 1 se prescribe que: "Los Estados miembros se asegurarán de que los datos PNR proporcionados por las compañías aéreas a la UIP se conservan en una base de datos de la Unidad durante un plazo de cinco años a partir de su transmisión a la UIP del Estado miembro en cuyo territorio tenga su punto de aterrizaje u origen el vuelo".

Este artículo aparece como una cláusula que corrobora el interés de la UE por garantizar el derecho al olvido estableciendo un plazo máximo para la conservación de los datos. Para reforzar esta garantía en el apartado 2 de dicho art. 12 se dispone que al finalizar un plazo de seis meses desde la transmisión de datos PNR mencionada en el apartado 1, todos los datos PNR deberán ser despersonalizados mediante enmascaramiento de los siguientes elementos que podrían servir para identificar directamente al pasajero al que se refieren los datos PNR:

a) nombre(s) y apellido(s), incluidos los de otros pasajeros que figuran en el PNR y número de personas que figuran en el PNR que viajan juntas;
b) dirección y datos de contacto;
c) rodos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, o a cualquier otra persona;
d) información sobre viajeros asiduos;
e) observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, y
f) toda la API (información anticipada sobre los pasajeros) recopilada.

Señala también el apartado 3 del art. 12 que al finalizar el período de seis meses mencionado en el apartado 2, solo se permitirá la divulgación de los datos PNR completos cuando:

a) se crea razonablemente que es necesario a los efectos establecidos en el artículo 6, apartado 2, letra b), y
b) haya sido aprobado por:
   i) una autoridad judicial, u
   ii) otra autoridad nacional competente para verificar si se cumplen las condiciones para la divulgación conforme al derecho nacional, con sujeción a la información y revisión a posteriori del responsable de la protección de datos de la UIP.

Asimismo se contempla en el apartado 4 del art. 12 que los Estados miembros se asegurarán de que los datos PNR sean suprimidos de modo permanente al finalizar el período a que se refiere el apartado 1. Esta obligación se entenderá sin perjuicio de aquellos casos en que se hayan transferido datos PNR específicos a una autoridad competente y se estén utilizando en el marco de un asunto específico a efectos de prevenir, detectar, investigar o enjuiciar los actos de terrorismo o delitos graves, en cuyo caso la conservación de los datos por la autoridad competente se regirá por el derecho nacional.

La disposición más importante de esta Directiva en relación con la garantía del *habeas data* se haya incluida en su art. 13. En dicho artículo se establece la plena garantía de los derecho ARCO consagrados por las normas de la UE y de los Estados que la integran (art. 13.1). Por tanto el *habeas data* está plenamente consagrado en este artículo. Se desprende de ello que medidas de seguridad y el tratamiento de la información policial con vistas a evitar posibles acciones criminales, en ningún momento podrán menoscabar las garantías de protección de datos establecidas en el marco de la UE.

En el apartado 4 de dicho art. 13 se afirma también que los Estados miembros prohibirán el tratamiento de datos PNR que revele el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona. En el caso de que la UIP reciba datos PNR que revelen tal información, los suprimirá inmediatamente.

En definitiva, se ofrece una garantía general del sistema consistente en la obligación de los Estados de la UE para velar por que sus UIP apliquen las medidas y los procedimientos técnicos y organizativos adecuados para

garantizar el elevado nivel de seguridad correspondiente a los riesgos que entrañen el tratamiento y las características de los datos PNR (art. 13.7).

6. CONCLUSIÓN

Las nuevas normas europeas de protección de datos, son el resultado de un largo y arduo proceso de elaboración. En particular, el *iter legis* del Reglamento ha sido especialmente problemático, por afectar a valores e intereses públicos y privados que rebasan el ámbito europeo, para adquirir una dimesión planetaria. El texto final ha debido superar las tentativas de mediatización de determinados *lobbies* ya que su contenido afecta a intereses de importantes grupos de presión multinacionales. La redacción de su normativa ha sido fruto de acuerdos, transaciones y compromisos por parte de las instancias europeas que han intervenido en su elaboración y aprobación. Por tal motivo, no han faltado valoraciones críticas sobre la calidad normativa de dicho Reglamento. Se ha denunciado que: "el Reglamento es complejo, burocrático y en muchos puntos confuso. De difícil comprensión para el ciudadano medio en lo que debiera ser una norma que debiera haberse inspirado en la claridad como eje imprescindible para la autodeterminación informativa y la seguridad jurídica"[21].

Estas consideraciones críticas, aunque se hallan fundamentadas, no deben dejar paso al pesimismo respecto a la futura eficacia del nuevo marco europeo de tutela de los datos personales. Determinadas formulaciones imprecisas y equívocas de esta norma, podrán ser ulteriormente enmendadas por los desarrollos legislativos de las normativas nacionales europeas. Tampoco puede omitirse la importancia de los jueces y tribunales que al aplicar esta normativa en los casos concretos pueden contribuir a subsanar algunos de sus planteamientos. No huelga recordar que, como se ha indicado en ocasiones, el Derecho informático debe gran parte de su desarrollo a su dimensión "pretoriana", es decir, que han sido los jueces quienes han contribuído de forma decisiva a actualizar y corregir determinadas normas reguladoras de esta materia y a colmar las lagunas que continuamente se producen en ese *perpetuum mobile* en que la protección de los datos personales consiste[22].

[21] J. LOPEZ CALVO, "Un Reglamento poliédrico que necesita un acercamiento poliédrico", en el vol. col., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* cit., pp. 81-82.

[22] Cfr., A. E. PEREZ LUÑO, *Libertad informática y leyes de protección de datos personale*s, en colab. con M. Losano y M. F. Guerrero Mateus, Centro de Estudios Constitucionales, 1989, Madrid, pp. 57 ss.

Como balance de las nuevas disposiciones de la UE en materia de protección de datos puede afirmarse que el Parlamento y el Consejo europeos han tratado de establecer unas medidas y mecanismos de garantía de los datos personales tratando que las mismas no se vean afectadas por la necesidad de los Estados de responder a los atentados terroristas y las actividades de la criminalidad internacional organizada. La grave inquietud cívica y política que motivaron los últimos atentados terroristas perpetrados en Europa por organizaciones vinculadas al fundamentalismo islámico han creado un síndrome de alarma entre los ciudadanos de Europa. Hace algunos años el sociólogo alemán Ulrich Beck[23] definió a las sociedades actuales como "sociedad del riesgo". En los momentos actuales parece que nos hallamos ante una situación en la que podría hablarse de unas "sociedades del miedo". Esta nueva circunstancia obliga a los poderes públicos europeos a tomar medidas de protección y seguridad, pero ese tipo de medidas no puede vaciar de contenido las garantías de la libertad que constituyen el fundamento axiológico de la propia UE. Por ello, en los textos aquí analizados se advierte esa búsqueda de un equilibrio adecuado entre las medidas de seguridad que requieren las sociedades actuales para luchar contra el terrorismo y la criminalidad y la tutela de las libertades que, en las sociedades tecnológicas europeas, tiene un capítulo de decisiva importancia en la garantía de los datos personales.

El otro aspecto importante de la normativa reseñada, es el que atañe a la preocupación constante de la UE por mantener una normativa jurídica de protección de datos actualizada, que responda a la constante evolución tecnocientífica. La UE ha sido sensible al impacto que sobre los derechos y libertades ejercen las Nuevas Tecnologías NT y las Tecnologías de la Información y de la Comunicación TIC[24]. En 1995 cuando se publica la directiva 95/46 UE las principales amenazas para la vulneración de los datos personales, fueron asumidas por ese texto normativo, en el que se quiso dar una respuesta jurídica a esos retos liberticidas. En el tiempo transcurrido desde aquella fecha

[23] U. BECK, *La sociedad del riesgo mundial: en busca de la seguridad perdida*, Trad. Cast., Paidós, Barcelona, 2008.

[24] Sobre las relaciones entre las NT y las TIC y los derechos humanos existe hoy una amplia bibliografía. Síntoma ejemplar de esas investigaciones es la obra realizada en el seno del Programa CONSOLIDER, a cargo de Antonio Enrique PÉREZ LUÑO, *Nuevas Tecnologías y Derechos Humanos*, Tirant lo Blanch, Valencia, 2014, en la que colaboran: Susana ALVAREZ, Miguel ALVAREZ ORTEGA, Ana GARRIGA, Rafael GONZALEZ-TABLAS, Fernando LLANO ALONSO y Cristina PAUNER. Vid, también, A.E.PEREZ LUÑO, *Los derechos humanos en la sociedad tecnológica*, Universitas, Madrid, 2012.

los avances tecnológicos y científicos han supuesto nuevas amenazas contra los derechos y libertades de los ciudadanos europeos, que han tenido proyecciones en la esfera de los datos personales. En el tiempo presente fenómenos tales como determinados programas de la neurociencia pueden invadir los estratos mas reservados de la persona. Además, existen ya experiencias de *Big-Data*, que permiten un uso y un control masivo de informaciones referentes a un número ilimitado de personas y a un número ilimitado de situaciones[25]. Ese almacenamiento masivo de datos personales, que a través de los algoritmos, pueden permitir todo tipo de tratamientos representan un gran reto para la tutela jurídica de dichos datos. Asimismo, en fecha muy reciente, para el estudio de las realidades y posibilidades de la robótica se ha acuñado un *Robot-Law*, que se ocuparía de la interacción entre los seres humanos y los robots y de la incidencia de la robótica en el ámbito de los derechos y libertades[26], en cuyo ámbito debe situarse la garantía de los datos personales.

A partir de ahora se abre el banco de prueba para comprobar en que medida la nueva normativa europea de protección de datos personales resulta eficaz para responder a los retos actuales de la tecnociencia. El legislador europeo, ha diseñado mediante las tres disposiciones normativas, a cuyo estudio se han dedicado estas reflexiones un marco jurídico, amplio y flexible, aunque no exentos de algunas deficiencias a las que se ha tenido ocasión de aludir, con el deseo de que resulte idóneo para la regulación, en el presente y en el inmediato futuro, de los principales impactos tecnológicos en los datos personales de los ciudadanos de la UE. Conjeturar sobre el éxito de esa pretensión es algo que escapa a la finalidad de este ensayo.

Enrique Pérez-Luño Robledo
Departamento de Derecho Procesal
Universidad de Sevilla
Avda. La Enramadilla, 18-20
41018. Sevilla
e-mail: eperezluno@us.es

[25] A. GARRIGA DOMINGUEZ, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua,* Dykinson, Madrid, 2015; Id., "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", cit., pp.108 ss.

[26] R. DE ASIS, *Una mirada a la robótica desde los derechos humanos*, Dykinson, Madrid, 2015.