http://dx.doi.org/10.22187/rfd2018n44a2
Doctrina

Alfonso Ortega Giménez y Juan José Gonzalo Domenech

Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea

New legal framework on the protection of personal date in the European Union

Novo quadro jurídico sobre proteção de dados pessoais na União Européia

Resumen: *Este trabajo versa sobre el impacto producido por la nueva legislación europea en materia de protección de datos. Se abordarán algunas de las principales novedades que trae consigo el nuevo Reglamento Europeo de Protección de Datos, (conocido también como Reglamento General de Protección de datos o RGPD) como la nueva figura del Data Protection Officer, los nuevos derechos y obligaciones promulgados, en especial, el derecho al olvido, el régimen sancionador y el futuro nuevo marco jurídico de la transmisión internacional de datos a terceros países, así como algunas menciones a la Directiva de protección de datos en materia penal y otra legislación relevante.*

Palabras clave: *protección, datos, reglamento, europeo, privacidad.*

Abstract: *This paper analyses the impact produced by new European legislation about data protection. It shall be studied some of the novelties that European Data Protection Regulation, (also known as General Data Protection Regulation or GDPR) such as new Data Protection Officer, new Rights and Obligations, specially, the Right to oblivion, sanctions regime and the new legal framework of cross-border data transfer. And some references to the data protection in criminal matters*

Alfonso Ortega Giménez: Doctor en Derecho. Profesor de Derecho Internacional Privado de la Universidad Miguel Hernández de Elche.
✉ *alfonso.ortega@umh.es*
Juan José Gonzalo Domenech: Colaborador del área de Derecho Internacional Privado de la Universidad Miguel Hernández de Elche.
✉ *jjgdjunior@gmail.com*

and other relevant legislation.

Keywords: *protection, data, regulation, European, privacy.*

Resumo: *Este artigo lida com o impacto produzido pela nova legislação europeia sobre a proteção de dados. Iremos abordar alguns dos principais desenvolvimentos que traz o novo regulamento europeu sobre a proteção de dados (também conhecido como Regulamento Geral de Proteção de Dados ou RGPD) como a nova figura da proteção de dados, os novos direitos e obrigações promulgadas, particularmente o direito a ser esquecido, o regime sancionatório e o futuro quadro jurídico novo para a transmissão internacional de dados para países terceiros, bem como algumas referências à diretiva sobre proteção de dados em matéria penal e outra legislação relevante.*

Palavras-chave: *proteção, dados, regulação, européia, privacidade.*

Recibido:
Aceptado:

Planteamiento

Durante el 2016 se publicaron los Reglamentos (UE) 2016/679 del Parlamento Europeo y el del Consejo del 27 de abril de 2016 relativos 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 (Reglamento General de Protección de Datos)[(1)], la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI[(2)] del Consejo, la Directiva (UE) 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[(3)], y la Decisión de ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU[(4)], además de numerosas guías de adecuación al RGPD[(5)] por lo que 2016 ha sido el año de la revolución normativa existente en materia de protección de datos personales a nivel europeo.

El objeto del presente trabajo es analizar algunas de las novedades introducidas por ambos textos normativos, en particular, por el Reglamento General de Protección de Datos Personales y ver la influencia de los tribunales, tanto nacionales como comunitarios, en la construcción de los derechos en ellos promulgados.

Novedades introducidas por la nueva normativa

La consecuencia directa que trae este nuevo Reglamento 2016/679 es la derogación de 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[6], con ya 17 años de vigencia desde su publicación, y la Directiva 2016/680 que deroga la Decisión Marco 2008/977/JAI del Consejo[7].

Nace con la necesidad de realizar una reforma de gran calado en la normativa comunitaria para elevar en la Unión Europea la exigencia legal de esta materia tan importante en la nueva "sociedad del dato".

A) Podemos destacar la obligatoriedad y la aplicación directa del Reglamento en los países de la Unión Europea, por lo que no necesita transposición y con ello, acelera la eficacia de la aplicación de la norma en los Estados. Esta novedad trae como consecuencia la creación de un mercado único digital. Según su art. 2 se establece que "El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

Y no se aplicará, en particular:

a) Al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión

b) A la actividad de las autoridades con fines de prevención o investigación de delitos o de protección de la seguridad pública,

c) A las actividades de los Estados miembros comprendidas en el ámbito de aplicación del capítulo

d) Ni al tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

B) Observamos que se fortalecen las obligaciones de información a los interesados (artículos 13 y 14 del RGPD). Una de las modificaciones introducidas por el Reglamento deriva de la aplicación del principio de transparencia, ya que se refuerza la información que se debe facilitar a los titulares de los datos, tanto en el supuesto de que los datos se recaben directamente del interesado como si los datos se obtienen de otra fuente.

En ambos supuestos deberá facilitarse al titular del dato, además de la información obligatoria ya establecida en la normativa española actual, información, entre otros aspectos, sobre: la base jurídica del tratamiento, la intención de realizar transferencias internacionales, el plazo de conservación de los datos o el derecho a la portabilidad de los datos;

C) Por otra parte, respecto al interesado cuyos datos se han obtenido de otra fuente, la información anteriormente indicada deberá facilitarse en el plazo máximo de un mes (en lugar de los tres meses indicados en la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal o LOPD[8]) a contar desde la primera comunicación o momento el que se comuniquen los datos de los interesados a un destinatario, salvo que la información ya fuese anteriormente conocida por el titular del dato o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado.

Es decir, la obligación de información se refuerza drásticamente, lo cual exigirá un esfuerzo considerable para los responsables del fichero de cara a adecuar sus cláusulas de información a los interesados, especialmente en materia de conservación de datos y transferencias internacionales, debiendo ser muy cautelosos en la forma de facilitar la información al objeto de poder acreditar con posterioridad que la misma ha sido facilitada;

D) Otra novedad para todas las empresas será la obligación de notificar a los reguladores fallos de seguridad en el plazo de 72 horas desde que tengan conocimiento de los mismos y, en determinadas circunstancias a los titulares de los datos (artículo 33 del RGPD). Se hace más estricta la necesidad de consentimiento de los afectados para el tratamiento de sus datos, limitando el consentimiento tácito y creando nuevas categorías de datos sensibles como los datos biométricos que requerirán un consentimiento reforzado.

Si existe una probabilidad alta de riesgo para los derechos y libertades de los individuos, se deberá igualmente notificar a los afectados tan pronto como sea posible y sin dilaciones injustificadas. Se puede evitar tener que comunicar el incidente a los afectados, si se han establecido previamente medidas técnicas y organizativas y se han aplicado a los datos afectados por la brecha, haciéndolos ininteligibles para accesos no autorizados, como puede ser el uso de la encriptación, o si el controlador ha tomado medidas posteriores que eliminan la probabilidad que se materialice ese alto riesgo o que le exija esfuerzos desproporcionados, en cuyo caso puede ser sustituida por una comunicación pública o similar en la que los afectados puedan ser debidamente informados;

E) El Reglamento matiza las cuestiones que deberá regular el contrato que se formalice entre el responsable y el encargado del tratamiento (artículo 28 del RGPD). Entre otros aspectos, establece la obligación del encargado de colaborar con el responsable para que éste cumpla de la mejor manera posible las obligaciones que le corresponden frente a los interesados, regula la obligación del encargado de cooperar y facilitar las obligaciones de seguridad que corresponden al responsable, o la obligación de facilitar información sobre la gestión de seguridad que ha realizado para a la vez el responsable pueda probar de la mejor manera posible el cumplimiento de las medidas de seguridad que le corresponde. Vemos, pues, que se amplía el ámbito subjetivo de responsabilidad con relación a los prestadores de servicios o encargados de tratamiento.

Se crea en este contexto el concepto de ventanilla única. Esto significa que, en caso de que el responsable o el encargado del tratamiento tengan múltiples establecimientos dentro de la UE, la autoridad supervisora del Estado Miembro donde el responsable/encargado tenga su "establecimiento principal" será la competente para supervisar y hacer cumplir la normativa de protección de datos en toda la UE. Mediante la creación de esta Autoridad de Control, el vicepresidente de la Comisión Europea afirma que se conseguirá un ahorro de 2.300 millones de euros al año por la reducción de burocracia.

Se puede hablar de una tendencia general del Reglamento a precisar el ámbito de colaboración entre el encargado y el responsable. En el mismo sentido jurídico se podría hablar de un desarrollo legal de las obligaciones de colaboración. La regulación anterior de la Directiva 95/46/CE no detallaba

expresamente estas obligaciones, como tampoco lo hace la LOPD. Sin embargo, en el RGPD las obligaciones de colaboración se explicitan claramente, a modo de un armazón jurídico de referencia que favorece la seguridad jurídica y la protección efectiva de los derechos fundamentales.

Además, el Reglamento Europeo establece la posibilidad de que la Comisión o la autoridad de control adopten unas cláusulas contractuales tipo en las que se regulen las obligaciones, a efectos de protección de datos, entre el responsable y el encargado de tratamiento, en las cuales podrán basarse los contratos formalizados entre responsable y encargado del tratamiento. No obstante, habrá que esperar al desarrollo de las mismas por la Comisión o autoridad de control de cara a determinar si es más conveniente la elaboración de las cláusulas *ad hoc* o adherirse a las cláusulas tipo;

F) El Reglamento Europeo ha introducido la figura del Delegado de Protección de Datos (DPO, en inglés. Artículos 37-39 del RGPD), imponiendo la obligatoriedad del nombramiento de un DPO a todos los organismos públicos –con la excepción de tribunales en aplicación de la función judicial– y a las entidades privadas, sean éstas consideradas responsables o encargados del tratamiento, cuyas actividades principales conlleven la "observación habitual y sistemática de interesados a gran escala" o el "tratamiento a gran escala de categorías especiales de datos".

El DPO deberá conocer profundamente las normas de protección de datos europeas, así como su práctica. Podrá ser un empleado de la compañía o actuar mediante un contrato de prestación de servicios. La compañía está obligada a apoyar al DPO en la realización de sus funciones, sin que esté sometido a las instrucciones de ningún estamento de la propia compañía, respondiendo únicamente ante "el más alto nivel jerárquico" de la misma. Como elemento más relevante, se prevé la prohibición expresa de destitución o sanción del DPO con causa en el desempeño de sus obligaciones. En el caso español, se ha preparado un sistema de certificación para obtener la cualificación como DPO siguiendo los criterios de la norma internacional ISO/IEC 17024:2012. Este sistema ha sido llevado a cabo por la Agencia Española de Protección de Datos (AEPD)[9], y ha sido la primera autoridad europea en desarrollar dicho esquema.

En cuanto a las funciones que tendrá el DPO, destacan el asesoramiento general dentro de la compañía en todo lo relativo a protección de datos personales, la supervisión del cumplimiento de la legislación y políticas de privacidad con especial atención a los riesgos asociados a las actividades que llevara a cabo la empresa, la elaboración de informes de evaluación de impacto de ciertos tratamientos de datos personales y la cooperación con las autoridades de control nacionales.

No obstante esto solo afectará a los siguientes supuestos:

(I) cuando el tratamiento sea realizado por una autoridad u organismo público, a excepción de los tribunales que actúen en su capacidad judicial;

(II) la actividad esencial del responsable de fichero o del encargado de tratamiento implique la monitorización regular y sistemática a gran escala de datos personales; o

(III) la actividad esencial de responsable de fichero o del encargado de tratamiento implique el procesamiento a gran escala de categorías especiales de datos o de datos relativos a antecedentes penales.

Con la incorporación de DPO podemos afirmar que se pretende dar una mayor fuerza a la figura del Responsable de Seguridad, que es la persona que actualmente se debe asignar en las organizaciones para velar por el correcto cumplimiento de la legislación española sobre protección de datos.

La diferencia más notoria entre el Responsable de Seguridad y el Delegado de Protección de Datos es la exclusividad de éste último en sus funciones, el DPO ya no será como hasta ahora la persona que se designaba como Responsable de Seguridad, ocurriendo que, sin apenas justificación, se elegía al informático o se autonombraba el administrativo al que su jefe le derivó informarse sobre cómo cumplir con la LOPD en la empresa, es por ello que esta nueva figura supone reforzar la cultura del *compliance* en materia de protección de datos (Lambert, 2016);

G) Establece numerosos principios que deben tenerse en cuenta a la hora de tratar con los datos personales y son compartidos con la Directiva relativa a la protección de datos personales para fines de prevención criminal (artículo 5 del RGPD):

1. Se dicen que los datos se trataran de forma lícita, con lealtad y transparencia.

2. Serán recogidos para fines determinados, explícitos y legítimos y no serán tratados para otros fines; es una limitación de la finalidad.

3. Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; minimización de datos.

4. Exactos y, si fuera necesario, actualizados.

5. Serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

6. Se garantizará una seguridad adecuada de los datos, incluida la protección frente a usos no autorizados. Prima la integridad y confidencialidad. La medida de seguridad que más ha destacado el RGPD es la obligación de cifrado (Fernández Burgueño, 2017).

7. Responsabilidad proactiva del responsable con el fin de que lleve a cabo las medidas oportunas para garantizar los principios anteriores (Villarino Marzo, 2013); llamado en el RGPD "privacidad por diseño". Consiste en la obligación de las organizaciones de anticiparse a los ciberincidentes, accidentales o deliberados, que razonablemente pudieran ocurrir, haciendo uso de una metodología que conduzca a la adopción de un conjunto de medidas adecuadas que aseguren –también, razonablemente– que están en condiciones de cumplir con los principios, derechos y garantías que el RGPD establece (Galán Cordero, 2017).

8. La protección de datos debe hacerse desde el diseño y por defecto: debido a sus riesgos y costes;

H) El consentimiento es la principal base legal legitimadora del tratamiento de datos personales (artículo 6 del RGPD). En la Directiva 95/46/CE se hablaba de consentimiento "inequívoco", mientras que la Comisión lo modificó en su propuesta por consentimiento "explícito". El Parlamento siguió la misma línea, mientras que el Consejo ha vuelto al consentimiento "inequívoco", reservando el "explícito" para tratamientos de datos sensibles, que permitan la elaboración de perfiles o para transferencias internacionales basadas en consentimiento (salud, origen racial, religión, vida sexual, etc.). Sin embargo, la cuestión terminológica pierde relevancia dado que el Reglamento incluye la definición de consentimiento, que se configura como una acción positiva o declaración. Por tanto, parece que el consentimiento tácito, basado en la inacción, perdería su operatividad. El responsable tendrá que ser capaz de demostrar que obtuvo el consentimiento necesario del titular de los datos personales (artículo 7 del RGPD).

Los interesados pueden oponerse a la realización de su perfil cuando la base legal que hubiera utilizado el responsable no fuera el consentimiento (por ejemplo, el interés legítimo). Es decir, no existiría ponderación entre los intereses personales del afectado y el interés legítimo del Responsable: la oposición se tendría que conceder en todo caso;

I) El ámbito de los menores es uno de los más delicados y agudos de los que se encuentran en la Protección de Datos, y sorprende la atención que se le ha prestado ya desde la Propuesta de Reglamento, no solo en sede de principios, como por ejemplo en los de calidad de datos y habilitación para el tratamiento, sino también en la regulación contenida en el artículo 8 del RGPD sobre "condiciones aplicables al consentimiento del menor en relación con los servicios de la sociedad de la información".

Estas normas pueden aplicarse también de forma análoga a otros ámbitos directamente relacionados con los niños, tales como el tratamiento de datos para disposiciones testamentarias, de salud o de ideología, religión y creencia de los menores. Así, en relación con la oferta directa de servicios de la sociedad de la información a menores, únicamente será lícito el tratamiento de los datos personales de menores de 16 años o, en caso de que el Derecho de

un Estado miembro disponga una edad menor, pero en ningún caso inferior a los 13 años, si dicho consentimiento resulta dado o autorizado por el titular de la autoridad parental sobre el niño (Díaz Díaz, 2016);

J) El nuevo Reglamento pretende unificar los criterios comunitarios para la imposición de sanciones, así como aumentar su cuantía para garantizar la mayor protección de un derecho fundamental como la privacidad (artículos 83 y 84 del RGPD).

Se amplía así el alcance de las sanciones contra los responsables y encargados del tratamiento que no cumplan con la normativa, y se faculta a las Autoridades Nacionales de Protección de Datos a imponer sanciones administrativas de hasta 20 millones de euros o el 4% de su volumen de negocios total anual para los casos de vulneración de los derechos de los interesados o incumplimiento de los dictámenes del órgano de control, transferencia de datos a un tercer país no seguro o vulneración de los principios sobre el tratamiento de datos personales. Se establecen multas de 10 millones de euros o el 2% del volumen global de negocio anual en caso de incumplimiento de las obligaciones del responsable, obligaciones del órgano certificador y de la autoridad de control. En ambos casos, se optara por la medida más cuantiosa.

A la hora de cuantificar la multa, deben utilizarse los siguientes criterios:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado.

Debido a la dureza de las medidas, puede crear en las empresas un efecto desalentador a la hora del trato de datos personales, y puede influir en la internacionalización del negocio.

Además, se reconoce el derecho de los interesados a presentar una reclamación a la Autoridad de Control nacional, así como su derecho a la tutela judicial efectiva ante los órganos jurisdiccionales de cualquier Estado Miembro;

K) la nueva normativa tiene por fin devolver el control de los datos personales a sus propietarios, y esto se manifiesta en los nuevos derechos que adquieren los ciudadanos (artículos 12-22 del RGPD):

I. Se le facilitará determinada información al interesado cuando la fuente de sus datos personales proceda o no del interesado dependiendo del supuesto.

II. Derecho de acceso del interesado: 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.

III. Derecho de rectificación: el interesado tendrá derecho a solicitar la rectificación de datos que considere inexactos o incompletos.

IV. Derecho de supresión (derecho al olvido): el interesado podrá pedir la supresión de los datos personales que le conciernan cuando concurra alguna causa que precise el reglamento. Abordaremos este derecho con más detenimiento.

V. Derecho a la limitación del tratamiento: el interesado podrá pedir la limitación en su uso de determinados datos personales una vez cumplida alguna de las condiciones que dicte la norma.

VI. El responsable está obligado a comunicar cualquier rectificación, supresión o limitación de los datos personales.

VII. Derecho a la portabilidad de datos: el interesado podrá recibir todos los datos que le incumban y que haya facilitado a otro responsable, y

transmitirlos a otro responsable sin que exista oposición por parte del responsable originario;

L) Códigos de Conducta o al someterse a una Certificación (artículos 41-44 del RGPD): En relación a los primeros, serán promovidos por los Estados Miembros, las autoridades de control, el Consejo Europeo de Protección de Datos y la Comisión, atendiendo a las peculiaridades de cada sector y de las pequeñas y medianas empresas. Las asociaciones quedan legitimadas para elaborarlos o adherirse a alguno ya existente, enmendarlo o modificarlo. Una certificación recomendada sería el Esquema Nacional de Certificación (Galán Cordero, 2017).

Si el tratamiento objeto del código no afecta a varios Estados Miembros sino que afecta a uno solo, será la autoridad de control de ese estado la encargada de supervisarlo, imponer las salvaguardas adecuadas, registrarlo y publicarlo. Pero si afecta a varios Estados, el encargado de supervisarlo y enmendarlo será el Consejo Europeo de Protección de Datos, que posteriormente dará traslado del mismo a la Comisión Europea para que declare en su caso, su validez en toda la Unión y lo publique.

La supervisión del cumplimiento del código, sin perjuicio de las competencias de la autoridad de control, puede ser llevada a cabo por una entidad independiente con un nivel de *expertise* adecuado al contenido del código y que haya sido acreditado para ello por la autoridad de control. Además de independencia y *expertise* deberá establecer procedimientos para asesorar a controladores y procesadores en el cumplimiento del código, monitorizar su cumplimiento, revisar periódicamente esas operaciones y establecer procedimientos y estructuras para atender las reclamaciones por el incumplimiento de las estipulaciones del mismo. Sin perjuicio de las competencias de la autoridad de control, deberá establecer medidas para el incumplimiento de las obligaciones reguladas en el Código, como pueden ser la exclusión o la suspensión;

M) Los Estados miembros, las autoridades de control, el Comité Europeo de Protección de Datos y la Comisión promoverán modelos de certificación, sellos o marcas que sirvan para demostrar cumplimiento con el RGPD. Las específicas necesidades de las microempresas y las PYMES deberán ser tenidas en cuenta. Será de carácter voluntario y no reducirá la responsabilidad

del cumplimiento con el RGPD por parte de controladores y procesadores de datos.

Serán otorgadas por entidades de certificación o por las autoridades de control. De otorgarla el Consejo Europeo de Protección de Datos, se denominará como certificación tipo "Sello Europeo de Protección de Datos". Se otorgará por periodos máximos de 3 años pudiendo ser renovada si se cumplen los requisitos para ello. El Consejo Europeo de Protección de Datos llevará un registro público con todas las certificaciones, sellos y marcas otorgados.

En relación con la entidad de certificación que emite y renueva los certificados, sellos o marcas, después de informar a la autoridad de control, deberá contar con un nivel adecuado de *expertise* en protección de datos. Cada estado decidirá quién otorga la acreditación a estas entidades de certificación, pudiendo ser:

- La autoridad de control competente.

- La Entidad Nacional de Acreditación denominado en acuerdo con el Reglamento (CE) Nº 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos, sin perjuicio de las competencias de la autoridad de control.

Quedan igualmente detallados los requisitos mediante los cuales se obtiene la condición de entidad de certificación y su renovación como máximo por periodos de 5 años. En el caso de incumplimiento por parte de la entidad de certificación, la acreditación podrá ser revocada (González-Calero Manzanares, 2016);

N) Transferencias internacionales de datos. Se mantiene y mejora el sistema instaurado en la Directiva 95/49/CE, existiendo unos supuestos exentos y mecanismos habilitantes (declaración de país con nivel adecuado de protección y transferencias con garantías, tales como, cláusulas contractuales tipo o reglas corporativas vinculantes (*Binding Corporate Rules*) Posteriormente, analizaremos el impacto de la jurisprudencia y la figura del *Safe Harbour*;

O) Se reformulan las competencias, funciones, poderes y condiciones generales de las autoridades de control estatales (en nuestro caso, la AEPD) Se crea un Comité Europeo de Protección de Datos y autoridades de control mediante el artículo 61 del RGPD. Sustituye al actual Grupo de Trabajo del Artículo 29. Se refuerzan y amplían sus competencias. Para los supuestos en los que un procesador o controlador se encuentre establecido en varios Estados Miembros, se establece que la autoridad de control del estado en el que radique el establecimiento principal pueda actuar como autoridad líder de control, regulándose el procedimiento de coordinación con el resto de autoridades. Se refuerzan los mecanismos de cooperación, asistencia mutua y actuación conjunta entre las diferentes autoridades nacionales de control. Para lograr la uniformidad en la aplicación del RGPD, se establece el principio de coherencia que obliga a las autoridades de control a cooperar entre ellas y cuando sea relevante, también con la Comisión Europea. Para lograrla, se establecen como mecanismos los Dictámenes del Comité Europeo de Protección de Datos y mecanismos de resolución de disputas entre autoridades de control por este mismo Comité;

P) En cuanto a la directiva 2016/680, su principal fin es garantizar la adecuada protección de los datos de las víctimas, testigos e investigados por la presunta comisión de delitos. Además, pretende armonizar la cooperación transfronteriza de la policía y los fiscales para combatir más eficazmente el crimen y el terrorismo en toda Europa.

La Directiva se estructura en 65 artículos divididos en 10 capítulos en los que se regulan cuestiones tales como los derechos de los interesados –los cuales coinciden con los del RGPD– las obligaciones de los responsables y encargados del tratamiento de los datos, las medidas de seguridad en el tratamiento o la creación, por parte de cada Estado Miembro, de una Autoridad Independiente de Control; y

Q) los Estados miembros tendrán que crear una Unidad de Información sobre los Pasajeros encargada de Gestionar los datos recopilados de las aerolíneas y almacenarlos durante cinco años. Tras los primeros seis meses, no figurarán lo datos de contacto. Transferir la información a las autoridades competentes e intercambiar los datos con las unidades de información de otros países de la UE y con Europol.

El almacenamiento de los datos se llevará a cabo según el caso y tan solo con fines de "prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves contemplados". Delitos como terrorismo, fraude, trata de blancas, blanqueo de capitales, explotación sexual, corrupción y tráfico ilícito de armas son los delitos que intenta prevenir. La norma será efectiva para los vueltos extracomunitarios, aunque los Estados podrán hacerla extensiva también a los intracomunitarios, siempre que se lo notifiquen previamente a la Comisión Europea.

Nuevos derechos otorgados por el RGPD: especial mención al Derecho al olvido

Nuevos derechos otorgados por el RGPD

1) Derecho de información (artículos 12 y 13 del RGPD) que se facilitará cuando los datos personales provengan del interesado: el responsable deberá facilitarle información relativa al propio responsable y, en su caso, representante, datos de contacto del DPO, los fines del tratamiento de datos, intereses legítimos en su caso, destinatarios, la intención de transferir los datos a un tercer país. Una vez obtenido los datos y, para cumplir con el principio de licitud y transparencia, se informara del plazo de conservación de los datos, existencia de los derechos de oposición, rectificación, supresión, limitación y portabilidad, posibilidad de retirar el consentimiento en casos específicos, derecho a presentar una reclamación ante la autoridad de control, requisito legal o contractual para comunicar los datos, la existencia de decisiones automatizadas, información del otro fin al que se destinen los datos.

2) Especialidades al anterior derecho en el caso de que provengan de una fuente diferente al del interesado como la fuente de la que provienen los datos y la comunicación de la obtención de los datos según esta forma (artículo 14 del RGPD).

3) Derecho de acceso del interesado (artículo 15 del RGPD): El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y derecho de acceso a los datos personales y a información como el fin a tratar, la categoría de datos personales, tipos de destinatarios, el plazo de conservación, existencia de los derechos de rectificación, supresión, limitación y oposición, el derecho

a realizar una reclamación, información sobre su origen, existencia de decisiones automatizadas, comunicación de las garantías en caso de transmisiones a terceros países y obtención de copia de los datos en un formato asequible.

4) Derecho de rectificación (artículo 16 del RGPD): El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

5) Derecho a la limitación del tratamiento (artículo 18 del RGPD): El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: impugnación del interesado mientras se investiga la exactitud de los datos, cuando el tratamiento sea ilícito y prefiera limitar su uso en vez de suprimirlos, necesidad de los datos para el interesado, verificación de legitimidad del responsable. Una vez limitados, tendrá que solicitar el responsable el consentimiento para su uso o para la protección de otras personas físicas o jurídicas o por razones de interés público por parte de la Unión o de un Estado. El interesado debe ser informado de la aplicación del derecho a la limitación.

6) Obligación de notificación relativa a la notificación o supresión de datos personales o su limitación (artículo 19 del RGPD).

7) Derecho a la portabilidad de los datos (artículo 20 del RGPD): El interesado tendrá derecho a recibir los datos personales que le incumban, proporcionados por el titular al responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando se haya basado en el consentimiento o se efectúe por medios automatizados. Se intentará realizar la transmisión de datos de responsable a responsable. No se aplicará el derecho cuando el tratamiento de datos se haga por misión en interés público. Es un derecho a recibir datos personales procesados por un responsable de tratamiento, para almacenarlo para uso personal adicional en un dispositivo privado, sin transmitirlo a otro res-

ponsable de tratamiento (Valdecantos Flores, 2017) pueden calificarse datos proporcionados por el titular:

> I. los datos facilitados activa y conscientemente por el interesado (dirección postal, nombre de usuario, edad, etc.), y
>
> II. Los datos observados son "proporcionados" por el interesado en virtud del uso del servicio o del dispositivo (historial de búsqueda, datos de tráfico o datos de localización). Sin embargo, los datos inferidos y derivados, por cuanto que son creados por el responsable sobre la base de los datos proporcionados por el interesado, no entrarán dentro del ámbito del derecho a la portabilidad de datos.

8) Derecho de oposición (artículo 21 del RGPD): el interesado podrá oponerse al tratamiento de los datos por motivos personales. El responsable dejará de tratar los datos salvo que alegue motivos imperiosos de interés público. Cuando el tratamiento de los datos esté enfocado al *marketing*, el interesado podrá siempre oponerse al tratamiento. Puede oponerse también cuando el tratamiento tenga fines históricos o estadísticos, pero no surgirá efecto si tiene como misión el interés público.

9) El interesado tendrá derecho a no estar sometido a un proceso totalmente basado en decisiones automatizadas, salvo si es necesario para la ejecución de un contrato, esté autorizada por el derecho de la Unión o el de los estados si se establecen unas medidas adecuadas o hay consentimiento explícito (artículo 22 del RGPD). El responsable debe tomar las medidas adecuadas para salvaguardar los derechos y no se aplicará en las categorías especiales de datos. Este "derecho" es diferente a otros que podemos encontrar en el RGPD, como el derecho de oposición (artículo 21), el derecho de supresión (artículo 17), o el derecho a la rectificación (artículo 16), puesto que este derecho no se ejerce por parte del afectado. No está claro cómo se caracteriza esta figura, dado que el apartado 1 lo configura como "derecho", mientras que el apartado 4 establece que las decisiones automatizadas "no se basarán en categorías especiales de datos". Es decir, lo configura como una "prohibición". Podría argumentarse que los legisladores habrían formulado el artículo 22.1 más como el artículo 22.4 si el derecho no fuese ejercido por el interesado (Mendoza y Bygrave, 2017).

Derecho al olvido

Mención especial merece uno de los mayores retos del S. XXI (Álvarez Caro, 2015) como es el 1) derecho de supresión, como se le reconoce en el artículo 17 del RGPD, 2) derecho al olvido, como se le conoce popularmente, o 3) derecho al "borrado" (Garriga Domínguez, 2016), como resulta más adecuado en la práctica. De reciente configuración en Europa pero ya reclamado anteriormente, la Agencia Española de Protección de Datos define El "derecho al olvido" como el derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima. Por tanto, ¿podemos considerarlo una especie de redención digital? (Leta Jones, 2016).

Este derecho no estaba expresamente recogido ni en la Directiva 95/46/CE, ni en la LOPD, pero eso no significa que no existiera hasta la Sentencia de la Gran Sala del Tribunal de Justicia de la Unión Europea de 2014 sobre el asunto C-131/12, sino que ese derecho ya existía con anterioridad, pero no fue interpretado correctamente.

> I. La actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en internet por terceros, almacenarla, y ponerla a disposición de los internautas, según un orden de preferencia determinado, debe considerarse un "tratamiento de datos personales" y el gestor de un motor de búsqueda debe ser responsable del tratamiento de esos datos.
>
> II. Cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro, que entiende que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro.
>
> III. El gestor de un motor de búsqueda está obligado a eliminar de la

> lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma licita.
>
> IV. Se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del públicos en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho públicos en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.

El nuevo Reglamento reconoce el derecho de esta forma: interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes como el fin del uso de los datos, retire el consentimiento, se oponga a su tratamiento, sea una obligación exigible por la Unión o por los Estados o los datos se hayan obtenido por una oferta de servicios de la sociedad de la información. Una vez tengan los responsables la obligación de borrar la información, deberán tener en cuenta la tecnología y los costes de una forma razonables. No existirá derecho al olvido cuando se haga en pro de la libertad de información, cumplimiento de una obligación

legal, necesaria para el interés público, información histórica o estadística, y para acciones de defensa.

Actualmente, existe una divergencia entre una reclamación realizada por la vía civil y la vía administrativa, siendo posible efectuar acciones indistintamente sin que una excluya a la otra derivada de las sentencias relacionadas con el derecho de supresión en la contradicción entre las SSTS 574/2016 y 210/2016. Ambas sentencias discuten sobre quién es el responsable del tratamiento de los datos, a lo que las salas dan respuestas contradictorias (De Miguel Asensio, 2016).

1. La STS 574/2016 estipula que el responsable del tratamiento de esos datos es quien gestiona técnica y administrativamente los medios para la indexación de la información, como es, en este caso, el motor de búsqueda. Y es la empresa matriz quien destina los medios para gestionarlo. La empresa filial no sería responsable si entre sus actividades principales no consta ninguna orientada a la indexación o almacenamiento de datos. No existiría tampoco corresponsabilidad al no existir unidad de negocio, ya que sus actividades están diferenciadas. Aunque sean representantes de la empresa matriz, es una sociedad con personalidad jurídica diferenciada y con objetivos diferenciados. Esta consideración se reduce en la jurisdicción C-A, cuyo objeto pueden ser las reclamaciones de los afectados por el medio indexador, así como las resoluciones de la AEPD en procedimientos de tutela de derechos en materia de protección de datos. Estas incidencias no pueden dirigirse contra la entidad filial, sino contra la matriz. Esta postura se ha reafirmado en posteriores sentencias[(10)] en las que se explicaba el procedimiento de ejercicio del derecho al olvido a la luz del artículo 26 del RGPD, llegando a la conclusión de que el responsable no es la filial, sino la matriz.

2. Por el contrario, la STS 210/2016 considera que el responsable del tratamiento es en la mayoría de casos la filial; ya que según el TJUE, interpretando la Directiva 95/46, no se exige para la aplicación del Derecho nacional que el tratamiento de los datos sea efectuado directamente por el propio establecimiento (la matriz) sino que se halle en las actividades de este. Considera que las actividades de la matriz y de la filial están ligadas; porque la filial, aun no dedicándose directamente a

> la indexación de la información, realiza actividades de promoción del medio de indexación o almacenamiento; además de ofrecerle los recursos económicos, sin importar la forma jurídica de la filial. Por lo tanto, la filial y la matriz son corresponsables del tratamiento de datos, y está legitimada pasivamente para ser parte demandada en los litigios seguidos en España en que los afectados ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición.

Resumiendo los problemas procesales y de competencia internacional, la sentencia de la sala primera explica que las sentencias no son contradictorias; ya que ambos casos están regidos por normas y principios totalmente diferentes, por lo que son complementarios en el siguiente sentido: para los casos respecto a procedimientos de tutela de derechos en materia de protección de datos, el responsable será la matriz extranjera. Para el ejercicio en un proceso civil de sus derechos; lo será también la filial nacional. La postura adoptada por el TS está fundamentada en el alto coste que supondría litigar contra una persona jurídica en el extranjero; aparte, está postura tiene el objetivo de favorecer a la parte débil (consumidor) en las transacciones internacionales de flujos de datos, permitiendo al afectado litigar en su lugar de residencia y sobre la base de su derecho nacional(11).

Transferencias internacionales de datos: del *Safe Harbour* al *Privacy Shield*

Régimen jurídico previsto en el RGPD

El nuevo régimen del RGPD está recogido en el Capítulo IV, y viene a sustituir el régimen basado en principios y excepciones de la Directiva 95/46/CE por un capítulo de siete artículos en los que se recoge el principio de prohibición general de transferencias internacionales (artículo 44); las transferencias realizadas bajo una decisión de adecuación (artículo 45); las transferencias realizadas mediante las garantías adecuadas (artículo 46); el régimen de las normas corporativas vinculantes (artículo 47); transferencias o comunicaciones no autorizadas (artículo 48); excepciones (artículo 49), y cooperación internacional (artículo 50).

La finalidad del RGPD es garantizar que sus normas ofrezcan el máximo nivel de protección a los titulares del derecho fundamental a la protección de

datos mediante una norma que reduzca la fragmentación jurídica y aumente la seguridad jurídica por la introducción de un conjunto de normas básicas unificadoras, de modo que en la práctica se impida su incumplimiento o menoscabo a través de conductas que distorsionen o desfiguren el régimen protector de las transferencias internacionales de datos, y con ello, del mercado interior.

Se ha reflejado en el RGPD la importancia de las transferencias de los flujos de datos a terceros países para la expansión del comercio (Oster, 2017) y de la cooperación internacional, pero las transferencias internacionales de datos no deben menoscabar el derecho a la protección de datos de los particulares(12).

Por ello, el nuevo régimen de las transferencias internacionales de datos del RGPD tiene una doble razón de ser (Pinar Mañas, 2016): por un lado, el flujo transfronterizo de datos es no solo imprescindible en la actualidad, sino que aumenta día a día; y por el otro, intentar restringir sin razones tales flujos de datos en pos de la protección de datos está abocado al fracaso.

El nuevo RGPD ha venido a subsanar este problema por la eficacia directa que disfrutan los Reglamentos europeos, y reforzando también el régimen de las transferencias, aumentando las garantías que se deben asegurar para llevarlas a cabo. No se limita solo a regular las transferencias con una mera decisión de adecuación; sino que también incluye normas claras para posibilitar transferencias mediante garantías adecuadas, transferencias mediante normas corporativas vinculantes, además de contemplar significativas excepciones para dar viabilidad práctica a situaciones específicas (Díaz Díaz, 2016).

El principio general de las transferencias es la prohibición, que podrá ser levantada si, prácticamente, cumple todas las obligaciones que manda el RGPD; en especial, las consistentes en garantías en las ulteriores transferencias. Como norma general, esa transferencia será autorizada mediante una decisión de adecuación que certifique que ese país, región, u organización internacional tiene un "nivel de protección adecuado". Las decisiones de todos los Estados que gozan de una decisión de adecuación –excepto la de EE.UU. – fueron modificadas por la Decisión de ejecución 2016/2295 de la Comisión, de 16 de diciembre de 2016; en las que se añadieron mayores controles por parte de la Comisión a los países con el nivel de protección ade-

cuado respecto a su ordenamientos jurídicos.

En caso de que no exista una Decisión de adecuación, solo se podrán transferir datos personales a un tercer Estado u organización si se hubieran ofrecido las garantías adecuadas y los derechos exigibles.

Los medios por los cuales se pueden aportar esas garantías son:

a) Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) Normas corporativas vinculantes;

c) Cláusulas tipo de protección de datos adoptadas por la comisión o autoridad de control y aprobadas por la comisión;

d) Un código de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los afectados, o

e) Un mecanismo de certificación, con los mismos compromisos que la medida anterior.

La Decisión de ejecución 2016/1250 del 12 de julio: el *Privacy Shield*

En 2015, la STJUE de la Gran Sala sobre el asunto C-362/14, caso *Schrems* anula la Decisión de la Comisión de 26 de Julio de 2000 (conocida como *Safe Harbour*) porque constató que Estados Unidos no puede ser considerado un tercer país que garantice un nivel de protección adecuada. El puerto seguro era una institución jurídica que permitía a las empresas la transmisión de datos hacia sociedades en EE.UU., cumpliendo una serie de principios Como referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), transferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados). Dichos principios son complementados con las “preguntas más frecuentes”, básicamente referidas

a tipos específicos de datos o tratamientos (García de Pablos, 2016).

El *Privacy Shield* es un mecanismo de autocertificación de empresas estadounidenses en el que se permite la transferencia de datos a las empresas que hayan sido certificadas mediante el cumplimiento de unos requisitos de seguridad y el cumplimiento de unos principios avalados por el Departamento Federal de Comercio. Las empresas certificadas se incluirán en una lista publicada por las autoridades estadounidenses en las que se muestran a todas las empresas que han superado el proceso de autocertificación. Esas empresas deberán renovar anualmente su autocertificación. Del mismo modo, deberán tomar medidas para verificar que las políticas de privacidad que han publicado se ajustan a los principios y se aplican.

El nuevo mecanismo sustitutorio fue aprobado mediante la Decisión de ejecución 2016/1250 el 12 de julio y de aplicación el 1 de agosto. La estructura de la nueva Decisión consta de solo seis artículos, pero de 155 considerandos y siete anexos donde se recogen los compromisos adquiridos por los organismos estadounidenses.

El *Privacy Shield* se aplica tanto a los responsables como a los encargados del tratamiento, si bien éstos deben estar obligados, por contrato, a actuar únicamente siguiendo instrucciones del responsable del tratamiento de la Unión Europea y asistir a este último a responder a las personas físicas que ejerzan sus derechos con arreglo a los siguientes principios (Pérez Cambero, 2017):

1. Principio de notificación/Derecho a ser informado:

Las empresas estadounidenses estarán obligadas a informar a los titulares de los datos sobre los aspectos clave en el procesamiento de sus datos de carácter personal (tipos de datos recopilados, propósito del procesamiento de los datos, derechos de acceso a la información y condiciones de transmisión o cesión de dichos datos a un tercero, medios de contacto con la empresa, órgano de resolución de controversias, APD de EE.UU.) además de diversas obligaciones formales (I. su adhesión al *Privacy Shield* y la indicación del enlace a la lista de entidades adheridas al mismo; II. los tipos de datos que se han recogido; III. el compromiso que tiene la entidad de cumplir con dichos principios; IV. la finalidad para la cual se recogen los datos; V. el procedimiento para contactar con la entidad para presentar reclamaciones y quejas).

2. Principio de elección/Derecho de elección:

Las empresas estadounidenses deberán obtener el consentimiento formal por parte de los ciudadanos antes de ceder sus datos personales sensibles a entidades terceras o se utiliza para un fin distinto por el que se recabaron los datos en un principio.

3. Principio de seguridad:

Las empresas estadounidenses deberán evaluar los riesgos de seguridad en el tratamiento de la información de carácter personal y deberán implantar medidas de seguridad que mitiguen al máximo riesgos como pérdidas, mal uso, acceso no autorizado, revelación, alteración o destrucción de estos datos. En el caso de que la entidad subcontrate a un tercero de un servicio determinado, se le deberá exigir un nivel de seguridad equivalente al requerido por la entidad para la protección de la información de carácter personal tratada.

4. Principio de integridad y limitación de la finalidad:

Las empresas estadounidenses deberán garantizar la integridad de los datos personales obtenidos; el titular de los datos solo deberá ser revelado en los casos en que esto sea imprescindible. La limitación de la finalidad de los datos implica que los datos de carácter personal recabados deben ser relevantes para los fines del tratamiento. Únicamente se permite guardar los datos personales en tanto resulten necesarios para el propósito del tratamiento. A dichas empresas se les permitirá conservar datos durante periodos más prolongados exclusivamente en caso de que los necesite para determinados fines en particular, tales como archivo por interés público, periodismo, literatura y arte, investigación científica o histórica, o para análisis estadístico (los mismos que se recogen en el RGPD).

Si el nuevo fin es sustancialmente distinto, la empresa sujeta al Escudo de Privacidad solo podrá usar sus datos si no se pone ninguna objeción o, en caso de tratarse de datos sensibles, si da su consentimiento. Si el nuevo fin está bastante relacionado con el original, su uso es permisible. Existe el derecho a elegir si los datos enviados a una empresa sujeta al escudo pueden transferirse a otra empresa, sea de EEUU o no. Si los datos son enviados a otra empresa para tratarlos en su nombre, ésta deberá suscribir un contrato con la

segunda empresa con las mismas garantías que ofrece el Escudo. La responsabilidad de la empresa receptora es extensible a la empresa sujeta al Escudo.

5. Principio de acceso/Derecho de acceso y rectificación de sus datos:

Las empresas estadounidenses deberán informar a los titulares de los datos sobre el contenido de los datos que obran en su poder y deberá facilitarles el acceso a dichos datos en un plazo de tiempo razonable, salvo que suponga un esfuerzo desproporcionado. Se podrá solicitar a la empresa que los corrija, los cambie o los elimine si no son exactos, están desfasados o han sido procesados infringiendo las normas del Escudo de Privacidad. La empresa deberá también confirmar si guarda y procesa o no sus datos personales. Las peticiones de acceso a su información personal podrán ser efectuadas por los ciudadanos en cualquier momento. Por lo general, no se obliga a dar ninguna razón acerca de los motivos por los que desea acceder a sus datos; no obstante; la empresa podrá pedirle que lo haga si su solicitud es demasiado genérica o vaga.

6. Principio de responsabilidad para transmisiones licitas:

Como elemento común, se pueden transmitir datos a terceros de manera lícita solo si existe justificación expresa.

Si se va a transferir los datos a un tercero responsable de los datos, deberán cumplir los principios de notificación y opción. Las entidades deberán requerir, a través de un acuerdo por escrito, que las terceras partes que reciban los datos personales, otorguen el mismo nivel de protección que el que proporciona el *Privacy Shield*.

Si se realiza a un tercero que actué como encargado del tratamiento, la entidad deberá de asegurarse, entre otras, de que este tratará los datos únicamente para los fines para los que fueron recabados.

7. Principio de responsabilidad, aplicación y responsabilidad/Derecho a reclamar y ser indemnizado:

Las empresas estadounidenses deberán implantar sistemas de verificación del cumplimiento de los principios del *Privacy Shield* y deberán infor-

mar de su cumplimiento de manera anual por medio de la renovación de su autocertificación, donde deberán acreditar las acciones que han adoptado para ceñirse a los principios del *Privacy Shield*. En el caso de que las empresas afectadas no demuestren el cumplimiento de dichos requerimientos, saldrán de la lista de empresas adheridas al *Privacy Shield* y estarán sujetas a sanciones económicas.

Si se considera que se han vulnerado los derechos y ha recibido un perjuicio, se tiene derecho a reclamar:

a) Ante la propia empresa estadounidense sujeta al Escudo de Privacidad. La empresa debe responder en un plazo de 45 días desde la recepción de la reclamación. La respuesta deberá establecer si la reclamación tiene o no fundamento y, en caso afirmativo, qué recurso aplicará la empresa como solución

b) Mediante un mecanismo de recurso independiente, como la RAL o ante la APD. La RAL es un procedimiento privado de resolución alternativa de litigios que debe ofrecer la empresa sujeta al Escudo. Puede ejercerse en la UE o en EEUU. También se puede optar por una APD europea.

c) Ante el Departamento de Comercio de los EE. UU (aunque únicamente a través de la APD). Este examinará su reclamación y responderá a su APD en un plazo de 90 días. El Departamento de Comercio también podrá remitir las reclamaciones a la Comisión Federal de Comercio (o al Departamento de Transportes).

d) Ante la Comisión Federal de Comercio de los EE. UU. (o el Departamento de Transportes de los EE. UU. Si la reclamación se refiere a una compañía aérea o una agencia de viajes).

e) Ante el Panel del Escudo de Privacidad, solo después de que hayan fracasado las demás opciones de reparación. Es un "mecanismo de arbitraje" compuesto por tres árbitros neutrales. Sus decisiones son vinculantes y ejecutables ante los tribunales estadounidenses. El recurso al arbitraje podrá invocarse únicamente a través del Panel del Escudo de Privacidad, y con arreglo a determinadas condiciones. Sólo el consu-

midor puede ejercer esta medida. Para iniciar el procedimiento, hay que notificar formalmente a la empresa su intención de hacerlo. La notificación deberá incluir un resumen de los pasos previos para resolver su reclamación y una descripción de la supuesta infracción. El arbitraje tendrá lugar en EE.UU., pero el consumidor tendrá diversos derechos:

• Solicitar la asistencia de su APD para preparar su reclamación.

• Posibilidad de tomar parte en los procedimientos por teléfono o videoconferencia, por lo que no se requiere estar presente físicamente en los EE. UU.

• Posibilidad de obtener interpretación y traducción de documentos sin ningún coste del inglés a otro idioma.

Los costes arbitrales correrán a cargo de un fondo constituido para ello. El procedimiento terminará en el plazo de 90 días, y si se declara a favor del consumidor, ofrece medidas de reparación como acceso, corrección, eliminación o devolución de los datos personales. El Panel no puede resarcir económicamente, por lo que habrá que acudir a los tribunales estadounidenses para ello. Si no se está de acuerdo al resultado del arbitraje, puede recurrirse ante los tribunales. Si la reclamación se efectuara contra una autoridad pública estadounidense, se activa el mecanismo del *Ombudsperson*, un alto funcionario de EEUU independiente receptor de reclamaciones. La reclamación se efectuará en colaboración con la APD del Estado miembro.

8. Se prevén otros principios accesorios en casos especiales

Como los datos sensibles, periodísticos, responsabilidad subsidiaria, auditorias, información sobre viajes, productos médicos y farmacéuticos, información de registros públicos e información accesible al público, o solicitudes de acceso de las autoridades públicas.

Por la otra parte, el Congreso de EE.UU. adoptó la ley de recurso judicial que permite salvaguardar la protección de los derechos y datos provenientes de la Unión[13].

Tras la publicación y entrada en vigor de la decisión, el GT29 dictó las WP-245 y 246 con una serie de indicaciones para las empresas y los individuos, donde aparece la información para solicitar el proceso de certificación para el *Privacy Shield*; así como indicaciones previas a la transferencia de datos. Además, se ha acordado que las autoridades nacionales sean consideradas órganos centralizados de la UE en el que se tramitan solicitudes de reclamación relativas a los accesos por razones de seguridad nacional a datos transferidos a EE.UU. con fines comerciales.

Pero no todo es positivo en esta nueva decisión, la poca rigidez en las obligaciones impuestas a los Estados Unidos (Wolters Kluwer, 2016), el lenguaje ambiguo, poco claro, y difícil de entender en algunos aspectos debido a que muchos términos se interpretan de manera diferente en la UE y en los Estados Unidos (Bu-Pasha, 2017), y las nuevas reformas emprendidas por el nuevo gobierno de Estados Unidos han supuesto una pérdida de protección de la privacidad, como la *Executive Order on Public Safety*[(14)], que excluye la aplicación de la ley de protección de datos estadounidense a las personas extranjeras en Estados Unidos, o la derogación de la *rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"*[(15)]; aunque recientemente se ha nombrado al nuevo *ombudsperson*, cargo desinado a dirimir las reclamaciones relacionados con el *Privacy Shield*, cuya independencia se pone en entredicho.

Todas estas medidas dirigidas a mermar la privacidad en Estados Unidos afectan directamente a los datos personales exportados a las empresas estadounidenses. Por ello, el Parlamento Europeo ha dictado una resolución[(16)] donde ha lamentado las nuevas reformas estadounidenses y pide a la Comisión Europea medidas destinadas a asegurar los principios estipulados en la Decisión. Por estos motivos, debemos mantener una postura cautelosa respecto al cumplimiento por parte de la nueva administración estadounidense del Escudo de Privacidad e, incluso, temer por la supervivencia del escudo cuando en septiembre se procederá a la revisión conjunta de la Decisión.

Reflexión final

Una completa revolución jurídica-digital: así debemos catalogar, no solo por el Reglamento sino también por la gran batería de medidas –como puede ser la propuesta de reglamento de privacidad en las comunicaciones electrónicas[17]– que se aproximan para alzar a la Unión y, con ella a sus Estados miembros, a un nivel adecuado a las necesidades tecnológicas de las que somos testigos, siendo el actual año clave para la privacidad, puesto que es el periodo de adaptación a la normativa europea.

La consolidación de los nuevos derechos y posibilidades provocarán una mejor circulación de datos, un aumento de la seguridad jurídica, nuevos métodos de resolución de problemas y una regulación armonizada y vinculante directamente. Pero no debemos confiarnos: la tecnología avanza a un ritmo trepidante, mucho más que su reflejo en el marco legislativo de forma adecuada, no como se está llevando a cabo al otro lado del océano; por lo que no debemos bajar la cautela con esta reforma, sino aumentarla al mismo ritmo que el propio avance de la tecnología para que los nuevos retos que nos plantea la tecnología, como es el caso del *Big Data,* no suponga un agravio para el derecho fundamental a la protección de datos.

Referencias

Álvarez Caro, M. (2015). *Derecho al olvido en internet: el nuevo paradigma de la privacidad digital*. Madrid: Editorial Reus.

Bu-Pasha, S. (2017). Cross-border issues under EU data protection lawwith regards to personal data protection, *Information & Communications Technology Law*, 1-17. DOI: http://dx.doi.org/10.1080/13600834.2017.1330740

De Miguel Asensio, P. A. (2016). La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google. *Diario La Ley*, (8773), 1-16.

Díaz Díaz, E. (2016). El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones. *Revista Aranzadi Doctrinal,* (6), 1-22.

Fernández Burgueño, P. (2017). La obligación de cifrado de la información en el Reglamento Europeo de Protección de datos. *Diario La Ley*, (3), 1-24.

Galán Cordero, C. (2017). El esquema nacional de seguridad como mecanismo de certificación del reglamento europeo de protección de datos. *Diario La Ley*, (5), 1-17.

Garriga Domínguez, A. (2016). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*. Madrid: Dykinson.

González-Calero Manzanares, F. R. (2016). Primera aproximación al Reglamento General de Protección de Datos, *Elderecho.com*. Recuperado de http://tecnologia.elderecho.com/tecnologia/privacidad/Aproximacion-Reglamento-General-Proteccion-Datos-dia-europeo-proteccion-datos_11_912055001.html

Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. Nueva Gales: CRC.

Leta Jones, M. (2016). *Cntrl+Z. The right to be forgotten.* Nueva York: New York University.

Mendoza, I., y Bygrave, L. (2017). The Right not to be Subject to Automated Decisions based on Profiling. *University of Oslo Faculty of Law Research Paper*, (20).

Oster, J. (2017). *European and International Media Law*. Cambridge: Cambridge University.

Pérez Cambero, R. (2017) Aspectos más destacables de la Decisión de Ejecución 2016/1250 de la Comisión Europea, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. *Actualidad Administrativa,* (4), 17-29.

Pinar Mañas, J. L. (2016). Transferencias de datos personales a terceros países u organizaciones internacionales En J. L. Pinar Mañas, *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (pp. 431-461). Madrid: Reus.

Valdecantos Flores, M. (2017). El derecho a la portabilidad de los datos en el Reglamento General de Protección de datos. *Diario La Ley*, (2), 1-14.

Villarino Marzo, J. (2013). La privacidad desde el diseño en la propuesta de reglamento europeo de protección de datos. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, (32), 1-25.

Wolters Kluwer (2016). 'El Escudo de Privacidad' entre la UE y EE.UU. necesita mejorar, *Diario La Ley*, (8760), 1-3.

Jurisprudencia

España. Tribunal Supremo. Sala 3ª de lo Contencioso-Administrativo. Sección 5ª. Sentencia 574/2016 de 18, de febrero de 2016. Recurso 3330/2014.

España. Tribunal Supremo. Sala 1ª de lo Civil. Sentencia 210/2016, de 5 de abril de 2016. Recurso 3269/2014.

Unión Europea. Tribunal de Justicia de la Unión Europea. Gran Sala. Sentencia del 6 de octubre de 2015, *Maximillian Schrems*. Asunto C-362/14. ECLI:EU:C:2015:650.

Notas

[1] Unión Europea. *Diario Oficial* L 119/1. 5 de mayo de 2016.

[2] Unión Europea. *Diario Oficial* L 119/86, 4 de mayo de 2016.

[3] Unión Europea. *Diario Oficial* L 119/32, 4 de mayo de 2016.

[4] Unión Europea. *Diario Oficial* L 207/1, 1 de agosto de 2016.

[5] 1) "Guía Protección de datos y administración de fincas"; 2) "Guía para la elaboración de contratos entre responsables y encargados"; 3) "Guía del Reglamento General de Protección de Datos para Responsables del Tratamiento", y 4) "Guía para el cumplimiento del deber de información". Todas ellas disponibles en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_02_23-ides-idphp.php

[6] Unión Europea. *Diario Oficial* L 281/31, 23 de noviembre de 1995.

[7] Unión Europea. *Diario Oficial* L 350/60, 30 de diciembre de 2008.

[8] España. *BOE* núm. 298, de 14 de diciembre de 1999.

[9] Documento "Esquema de la Agencia Española de Protección de Datos de certificación de delegados de protección de datos". https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Certificacion/ESQUEMA_AEPD_DPD_PUBLICO_1.0.pdf

[10] España. Tribunal Supremo. Sala 3ª de lo Contencioso-Administrativo. Sección 6ª. Sentencia 1381/2016, de 18, de febrero de 2016. Recurso 641/2015; y Sentencia 1387/2016 Recurso 1075/2015.

[11] Idea recogida en la STJUE de 25 de octubre de 2011, *eDate Advertising y Martinez*, C-509/09 y C-161/10, y plasmada en el artículo 79.2 RGPD.

[12] *Vid*. Considerando 101 del RGPD.

[13] EE.UU. Judicial Redress Act. Public Law No: 114-126 (02/24/2016).

[14] EE.UU. Executive Order 13768. *Federal Register* 82, 1 de febrero de 2017.

[15] EE.UU. Public Law No: 115-22 (04/03/2017).

[16] (2016/3018(RSP)).

[17] COM(2017) 10 final.