Pre-print: Revista Crítica de Derecho Privado, La Ley Uruguay, n.º 15, 2018, págs. 205-250. ISSN 1510-8090

Convergencia entre sistemas normativos: el Reglamento General de Protección de Datos europeo y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (*)

Rosa Mª García Pérez
Profesora Titular de Derecho Civil
Delegada de Protección de Datos
Universidad de Granada

SUMARIO

RESUMEN: El presente trabajo analiza la incidencia del nuevo marco europeo (Reglamento 2016/679/UE) en el consenso de unos principios comunes en la región iberoamericana para la armonización de las legislaciones nacionales de la región en la protección del derecho fundamental a la protección de datos. En un entorno tecnológico

* Este trabajo se enmarca en el Proyecto I+D (Retos) DER2017-84748-R: Mercado Único Digital Europeo y Protección de los Consumidores: Perfilando los derechos de las partes en contratos de suministro de contenidos digitales [*EU Digital Single Market and consumer protection: Assessing parties rights in contracts of suply of digital contents*]. Investigador principal: S. CÁMARA LAPUENTE. Ministerio de Economía, Industria y Competitividad (MINECO).

global, la convergencia entre sistemas se erige en una pieza fundamental para la protección de los derechos y libertades de las personas y en un motor de desarrollo de la economía digital.

PALABRAS CLAVE: Convergencia entre marcos regulatorios de la privacidad; Reforma de la normativa europea de protección de datos: Reglamento General de Protección de Datos; Armonización del derecho a la protección de datos personales en la región iberoamericana: los Estándares de Protección de Datos Personales de los Estados Iberoamericanos.

ABTRACT: *This paper analyzes the impact of the new European framework on the consensus of common principles in the Ibero-American region for the harmonization of the national legislations of the region in the protection of the fundamental right to data protection. In a global technological environment, the convergence between systems becomes a fundamental piece for the protection of the rights and freedoms of people and an engine of development of the digital economy*.

KEYWORDS: *Convergence between regulatory frameworks of privacy; Reform of European Data Protection Rules: General Data Protection Regulation; Harmonization of the right to personal data protection in the Ibero-American Community: the Standards for Personal Data Protection the Ibero-American States*.

I. UNA NORMA EUROPEA CON CLARA VOCACIÓN UNIVERSAL, EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EUROPEO (RGPD)

Después de una dilatada tramitación legislativa, iniciada a principios del año 2012 y plagada de tensiones e intereses encontrados de grupos de presión, el 4 de mayo de 2016 el Diario Oficial de la Unión Europea publicaba el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE -Reglamento General de Protección de Datos- (en adelante, RGPD)[1]. Dicha norma entró en vigor a los 20 días de su publicación, aunque su efectividad quedaba aplazada hasta el 25 de mayo de 2018.

[1] .- Diario Oficial de la Unión Europea, L 119, de 4 de mayo de 2016, pp. 1 y ss.

A nadie se oculta que la revisión del marco europeo de protección de datos de carácter personal, emanado a mediados de los años noventa del pasado siglo, en un contexto bien diferente al actual, era una necesidad. En poco más de 20 años, hemos pasado de la revolución que supusieron los ordenadores a conectarnos con todo el planeta a través de internet; de ser meros receptores de información en la web a tener un papel dinámico y activo de interacción y colaboración con otros usuarios; de la conexión entre personas a un mundo en que cualquier objeto podrá estar conectado, recibiendo y transfiriendo información sin barreras espaciales o temporales, es lo que se ha dado en llamar el internet de las cosas o *internet of things (IoT)*; y avanzamos vertiginosamente hacia nuevos escenarios que vienen de mano de programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana o están diseñados para aprender por sí mismos de forma autónoma a través de su propia experiencia e interactuar con el entorno (inteligencia artificial, robotización y *machine learning*). A ello hay que añadir que la gestión y control inteligente de la información, de los datos, es hoy posible gracias a desarrollos tecnológicos (*cloud computing*, *big data*) que han incrementado exponencialmente las capacidades de su computación y procesamiento masivo, sus posibilidades de análisis estadístico y predictivo y abaratado el coste de su almacenamiento.

Estos fenómenos e innovaciones tecnológicas han convertido a los datos personales, como dice Franklin FOER, en un activo muy preciado que ha permitido construir "imperios pulverizando la intimidad"[2] y a la sociedad actual en un gran "panóptico digital", en palabras del filósofo Byung-Chul HAN[3]; una versión más avanzada y

[2] .- En un ensayo recientemente publicado en el que advierte de los efectos negativos del poder de las grandes tecnológicas, este periodista estadounidense señala: «Uno de los lugares comunes de nuestro tiempo es que los datos son el nuevo petróleo. En un principio esto parecía una hipérbole, pero hoy se antoja una descripción adecuada. Datos es una palabra anodina, pero aquello que representa no lo es en absoluto. Denota el registro de nuestras acciones: lo que leemos, lo que vemos, los lugares adonde nos desplazamos en el transcurso del día, lo que compramos, nuestra correspondencia, nuestras búsquedas en la red, los pensamientos que empezamos a teclear y después borramos. Con suficientes datos, resulta posible percibir correlaciones y descubrir patrones. El gurú de la seguridad informática Bruce Schneier ha escrito: "Los datos acumulados pueden pintar probablemente un cuadro mejor de a qué dedicas tu tiempo, ya que no han de depender de la memoria humana". Los datos implican una comprensión de los usuarios, un retrato de nuestra psique. Eric Schmidt alardeaba en cierta ocasión: "Sabemos dónde estás. Sabemos dónde has estado. Podemos saber más o menos lo que estás pensando"… Un retrato de una psique es algo muy poderoso. Permite a las empresas predecir nuestro comportamiento y anticipar nuestros deseos… En este sentido, los datos no se parecen al petróleo. El petróleo es un recurso finito; los datos son infinitamente renovables» (FOER, F., *Un mundo sin ideas. La amenaza de las grandes empresas tecnológicas a nuestra intimidad*, Ed. Paidós, Barcelona, 2017, p. 182)

[3] .- «La sociedad actual del control muestra una especial estructura panóptica… Lo que garantiza la transparencia no es la soledad mediante el aislamiento, sino la hipercomunicación. La peculiaridad del panóptico digital está sobre todo en que sus moradores mismos colaboran de manera activa en su construcción y en su conservación, en cuanto se exhiben ellos mismos y se desnudan. Ellos mismos se exponen en el mercado panóptico. La exhibición pornográfica y el control panóptico se compenetran. El exhibicionismo y el voyeurismo alimentan las redes como panóptico digital. La sociedad del control se consuma allí donde su sujeto se desnuda no por coacción externa, sino por la necesidad engendrada en sí mismo, es decir, allí donde el miedo de tener que renunciar a su esfera privada e íntima cede a la necesidad de exhibirse sin vergüenza…. Hoy, el globo entero se desarrolla en pos de formar un gran panóptico. No hay ningún afuera del panóptico. Este se hace total. Ningún muro separa el adentro y el afuera. Google y las redes sociales, que se presentan como espacios de la libertad, adoptan formas panópticas. Hoy, contra lo que se supone normalmente, la vigilancia no se realiza como ataque a la libertad. Más bien, cada uno se entrega voluntariamente a la mirada panóptica. A sabiendas, contribuimos

mejorada del prototipo de prisión perfecta ideado en el siglo XVIII por BENTHAM, dado que el control y vigilancia se ve favorecido de manera activa por los propios moradores de la prisión que, de forma voluntaria y creyéndose en libertad, se entregan a la mirada panóptica, exponiéndose y revelando continuamente información personal.

A los desafíos para la privacidad, intimidad y demás derechos y libertades de las personas surgidos de este escenario digital, que cosifica y cuantifica[4] prácticamente todo, se une un contexto normativo europeo diferente al existente cuando se adoptó la Directiva 95/46/CE. Y es que en este periodo la protección de datos se ha consolidado y fortalecido como derecho constitucional. De sus orígenes[5], con la adopción del Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981[6], para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, pasa a la Carta de los Derechos Fundamentales de la Unión Europea, a la que el Tratado de la Unión Europea -en la redacción consolidada por el Tratado de Lisboa- otorgó el mismo valor jurídico que a los Tratados y el artículo 16 del Tratado de Funcionamiento de la Unión Europea confirió la base para la elaboración de una normativa global de la Unión Europea sobre protección de datos personales.

---

al panóptico digital, en la medida en que nos desnudamos y exponemos. El morador del panóptico digital es víctima y actor a la vez. Ahí está la dialéctica de la libertad, que se hace patente como control» (HAN, B., *La sociedad de la transparencia*, Ed. Herder, Barcelona, 2013, pp. 94-95).

[4] .- En otro trabajo, el filósofo alemán Byung-Chul HAN advierte en este sentido: «La palabra "digital" refiere al dedo (digitas), que ante todo cuenta. La cultura digital descansa en los dedos que cuentan. Historia, en cambio, es narración. Ella no cuenta. Contar es una categoría poshistórica. Ni los tweets ni las informaciones se cuentan para dar lugar a una narración. Tampoco la *timeline* (línea del tiempo) narra ninguna historia de la vida, ninguna biografía. Es aditiva y no narrativa. El hombre digital digita en el sentido de que cuenta y calcula constantemente. Lo digital absolutiza el número y el contar. También los amigos de Facebook son, ante todo, contados. La amistad, por el contrario, es una narración. La época digital totaliza lo aditivo, el contar y lo numerable. Incluso las inclinaciones se cuentan en forma de "me gusta". Lo narrativo pierde importancia considerablemente. Hoy todo se hace numerable, para poder transformarlo en el lenguaje del rendimiento y de la eficiencia. Así, hoy deja de ser todo lo que no puede contarse numéricamente» (HAN, B., *"En el enjambre"*, Ed. Herder, Barcelona, 2014, p. 60).

[5] .- El derecho a la protección de los datos personales forma parte de los derechos protegidos al amparo del artículo 8 del Convenio Europeo de Derechos Humanos de 1950, que garantiza el derecho al respeto de la vida privada y familiar, el domicilio y la correspondencia y determina las condiciones bajo las cuales podrían ser aceptables las limitaciones a ese derecho.

[6] .- El Convenio n.º 108 del Consejo de Europa y su Protocolo Adicional de 2001 del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y los flujos transfronterizos de datos está siendo sometido hoy día a un proceso de revisión. Constituye hoy por hoy el único instrumento internacional vinculante ratificado por 51 países y está abierto a la adhesión de los Estados no miembros del Consejo de Europa, incluidos los países no europeos. Uruguay, fue el primer país no europeo que se adhirió en agosto de 2013. Ha sido ratificado por varios países no europeos de África (Senegal y Túnez). Varias solicitudes de adhesión (por ejemplo, Argentina, México y Marruecos) están en curso y varios países tienen calidad de observador (por ejemplo, Japón y Corea del Sur). En la actualidad ha sido sometido a revisión a través del Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 108), adoptado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018 y abierto a la firma a partir del 25 de junio de 2018.

A ello conviene añadir la labor desarrollada por el Tribunal de Justicia de la Unión Europea en la delimitación del derecho de protección de datos. En particular, conviene destacar tres hitos, casi coincidentes con la tramitación del RGPD:

- Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014 (Asuntos C-293/12 y C-594/12), conocida como *Digital Rights Ireland Ltd*, que declaró la invalidez de la Directiva 2006/24/CE, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas, por vulneración del derecho de proporcionalidad que se opone a una conservación generalizada e indiferenciada de datos de tráfico y localización de los usuarios.

- Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014 (Asunto C-131/12), conocida como Google/Agencia Española de Protección de Datos (en adelante, AEPD) y Mario Costeja, que reconoció y perfiló un nuevo derecho: el derecho al olvido.

- Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 (Asunto C-362/14), *Maximillian Schrems*/*Facebook Ireland Ltd*, a través de la cual se anuló el sistema *Safe Harbour* (Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000), que consideraba a Estados Unidos como un «puerto seguro» en relación con las transmisiones internacionales de datos de carácter personal, permitiendo a empresas estadounidenses la prestación de servicios y tratamiento de datos de europeos en su territorio a condición de que se adhirieran a determinados principios[7].

En este escenario, tecnológico y jurídico, se hacía imprescindible una profunda revisión del marco normativo europeo de protección de datos. Esta es la tarea que acomete el RGPD[8], que pretende dar una respuesta global a la protección de datos, tanto desde la perspectiva del titular de los datos (reforzando su posición de control) como desde la de quienes realizan actividades de tratamiento de datos personales. Conviene, no obstante, advertir que el RGPD no viene solo, es la pieza nuclear de un «paquete normativo de protección de datos» más amplio, que incluye otras normas sectoriales:

- Por un lado, dos normas aprobadas y publicadas el mismo día que el RGPD: la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril

[7] .- Sobre la decisiva influencia del TJUE en los Tribunales constitucionales y órganos jurisdiccionales de los Estados miembros, así como las consecuencias de las sentencias *Digital Rights Ireland Ltd* y *Maximillian Schrems*/*Facebook Ireland Ltd*, en las relaciones Unión Europea - Estados Unidos, vid. LÓPEZ AGUILAR, J.F., "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del Derecho europeo, y su impacto en la relación transatlántica UE-EEUU", *UNED. Teoría y Realidad Constitucional*, núm. 39, 2017, pp. 557-581.

[8] .- Son numerosas los trabajos y obras publicadas en España centradas en el estudio de ciertos aspectos concretos del RGPD, como estudios generales conviene consultar: AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, dir. por José Luis PIÑAR MAÑAS, Ed. Reus, Madrid, 2017 y AA.VV., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, coord. por José LÓPEZ CALVO, Ed. Wolters Kluwer España, Madrid, 2018.

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 del Consejo[9]; y 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[10].

- Por otro, dos normas cuya tramitación se ha iniciado, el futuro Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE, conocido como Reglamento sobre la privacidad en las comunicaciones electrónicas o Reglamento *E-Privacy*[11]; y la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE[12]. Ambas propuestas normativas fueron presentadas por la Comisión europea el pasado 10 de enero de 2017, y actualmente se está discutiendo en el Consejo de la Unión Europea, tras su paso por la Comisión y el Parlamento.

Ahora bien, una de las claves del nuevo modelo de protección de datos europeo es su clara vocación universal, tratando de implementar unas reglas que armonicen internacionalmente el nivel de protección y flexibilicen el flujo internacional de datos transfronterizos. No hay que obviar que, en un entorno tecnológico global, los flujos internacionales de datos abogan por una búsqueda de soluciones globales en materia de privacidad, de ahí que el reto sea alcanzar unos estándares internacionales de protección de datos personales que desemboquen en un instrumento normativo universal y vinculante y, en este sentido, la norma europea pretende constituirse en el modelo de referencia.

II. LOS ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS (EPDPEI)

Uno de los primeros reflejos de esta decidida propensión del RGPD a extender su radio de acción y constituirse en un referente a escala internacional ha sido la reciente adopción de los *Estándares de Protección de Datos Personales para los Estados Iberoamericanos* (en adelante, EPDPEI) en el seno de la Red Iberoamericana de

[9] .- En https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L0680

[10] .- En https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.119.01.0132.01.SPA

[11] .- En https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

[12] .- Accesible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0008&from=EN

Protección de Datos[13] .

Iberoamérica carece de un marco común o armonizado, siendo la situación de los países muy dispar, englobando situaciones que van desde países que carecen totalmente de un marco regulatorio en la materia; los que reconocen el habeas data en sus Constituciones; los regulan el acceso a la información pública; los que otorgan protección mínima a través de normativas sectoriales de consumo, salud o financiera; o cuenta con un avanzado régimen en materia de protección de datos, más o menos desarrollado o actualizado. En un reciente trabajo[14], los países se han agrupado entorno a cuatro bloques: países con legislación específica en materia de protección de datos (Argentina, Chile, Colombia, Costa Rica, México, Nicaragua, Perú, República Dominicana y Uruguay), países con legislación en materia de privacidad (Paraguay y Puerto Rico), países con legislación en materia de *habeas data* como garantía constitucional de salvaguarda de la autodeterminación informativa (Bolivia, Brasil, Ecuador, Guatemala, Honduras[15] y Panamá) y otros países (Cuba, El Salvador y Venezuela).

Por otra parte conviene poner de manifiesto que, aun cuando la influencia europea, principalmente a través de España y Portugal, constituye la referencia nuclear para muchos países, no cabe despreciar en otros países la confluencia en algunos países iberoamericanos de otros marcos normativos como el estadounidense, de carácter más sectorial, o el propio del entorno Asia–Pacífico, de la mano del denominado Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (FCEAP)[16].

---

[13] .- Su texto fue aprobado en el XV Encuentro de la Red, celebrado en Santiago de Chile los días 20 a 22 de junio de 2017. Se encuentra accesible en la web de la Red Iberoamericana de Protección de Datos*:* http://www.redipd.org/noticias_todas/2017/novedades/common/Estandares_Esp_Con_logo_RIPD.pdf#Texto%20en%20espa%C3%B1ol.

[14] .- Vid. AA.VV., *Protección de datos y habeas data: una visión desde Iberoamérica*, coord. por Daniel A. LÓPEZ CARBALLO. Agencia Española de Protección de Datos, 2015; obra que fue merecedora del Premios de Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos en su XVIII edición.

[15] .- Actualmente, el Congreso Nacional de Honduras está tramitando una Ley de Protección de Datos, vid., http://congresonacional.hn/index.php/2018/04/26/nota-de-ley-de-proteccion-de-datospresidente-del-instituto-de-acceso-a-la-informacion-publica-ley-de-proteccion-de-datos-personales-protegera-un-derecho-fundamental-como-lo-es-la-intimidad/ (acceso el 20 de junio de 2018).

[16] .- En relación con este último conviene saber que en 2004, los Ministros de las 21 economías del FCEAP avalaron el Marco de Privacidad, el cual establece principios de protección de datos de carácter personal y promueve la creación de instrumentos internacionales para proteger la privacidad de los individuos al mismo tiempo que facilitar el intercambio de información entre las economías. Destaca como uno de estos instrumentos el Sistema de Reglas de Privacidad Transfronteriza (*Cross-Border Privacy Rules*, CBPRs, por sus siglas en Inglés). Este sistema facilita a los responsables ubicados en distintas economías de Asia Pacífico transferir datos personales entre ellos, siempre y cuando las transferencias sean seguras de conformidad con el Marco de Privacidad. Desarrollado por las veintiuna economías miembros del Foro, el sistema de CBPRs se centra en un código de conducta voluntario de privacidad para las empresas de las economías participantes que operan en la región, basado en nueve Principios: prevención de daño, aviso, limitación de colección, uso , elección, integridad, salvaguardas de seguridad, acceso y corrección y responsabilidad. No obstante, dado que una efectiva protección de datos personales depende de la cooperación regional e internacional, se desarrolló el Acuerdo de Cooperación Transfronteriza en materia de Privacidad (CPEA, por sus siglas en inglés). Las organizaciones que deseen participar en este sistema deben someter sus reglas y políticas de protección de datos personales a la validación de terceros certificadores (*accountability agents*), a fin de garantizar que los datos personales

Esa fragmentación en los niveles de protección de datos personales resalta el valor de una iniciativa como la acometida en el seno de la Red Iberoamericana de Protección de Datos, dirigida al establecimiento de unos estándares adecuados para la protección de datos personales que armonicen la normativa en espacio iberoamericano, proporcionando garantías y seguridad a las personas y contribuyendo al desarrollo de la región en el marco de la actual economía digital globalizada.

Como analizaremos, los EPDPEI[17] siguen muy de cerca los principios y bases del RGPD[18] y pretenden servir de referencia a los países iberoamericanos, ya sea para futuras revisiones de su marco legal e institucional de protección de datos, ya sea para afrontar su regulación cuando aún no disponen de alguno, contribuyendo de esta manera al establecimiento de una reglas homogéneas e iguales garantías de protección en el ámbito iberoamericano. En concreto, sus objetivos explicitados en el propio artículo 1 de su texto son los siguientes:

1. *Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.*
2. *Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, así como entre los Estados Iberoamericanos, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.*
3. *Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos,*

---

estarán protegidos. Los terceros certificadores también se encuentran validados por el sistema. El CPEA es el primer acuerdo en su tipo en la región, para la cooperación transfronteriza en la vigilancia y cumplimiento de normas de privacidad y protección de datos de la región Asia Pacífico y, en especial, del Marco de Privacidad de APEC y del Sistema de Reglas de Privacidad Transfronteriza (CBPRs). El 12 de junio de 2017, Corea del Sur se convirtió en el último país en unirse oficialmente al Sistema de Reglas de Privacidad Transfronterizas (CBPRs) de la Cooperación Económica Asia-Pacífico, uniéndose a los Estados Unidos, Canadá, Japón y México. Hasta la fecha, veinte compañías (entre las que se encuentran Apple, Cisco, HP, IBM, Rackspace y Workday) han sido certificadas bajo el CBPRs.

[17] .- Un antecedente directo fueron los *Estándares internacionales sobre protección de datos personales y privacidad* (Resolución de Madrid), documento que se preparó a lo largo de un año por un Grupo de Trabajo encabezado por la Agencia Española de Protección de Datos (AEPD) y fue aprobado en 2009 por las Autoridades de Protección de Datos de 50 países reunidas en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en Madrid. En ellos se recogen distintos enfoques de legislaciones de los cinco continentes, que en cierta medida han sido recogidos por el RGPD. Pueden consultarse en *Revista Autocontrol*, n.º 148, pp. 8 a 14.

[18] .- Además del RGPD, en el Preámbulo de los EPDPEI se alude a la toma en consideración de otros instrumentos internacionales en materia de protección de datos personales, como son las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos; el Convenio número 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo; y el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (FCEAP).

mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.

4. *Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región.*
5. *Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia*.

Su texto, con un total de 45 artículos, se estructura en 26 considerandos y 10 capítulos:

Capítulo I: Disposiciones generales
Capítulo II: Principios de protección de datos personales
Capítulo III: Derechos del titular
Capítulo IV: Encargado
Capítulo V: Transferencias internacionales de datos personales
Capítulo VI: Medidas proactivas en el tratamiento de datos personales
Capítulo VII: Autoridades de control
Capítulo VIII: Reclamaciones y Sanciones
Capítulo IX: Derecho de indemnización
Capítulo X: Cooperación internacional

II. MEDIDAS ADOPTADAS POR EL RGPD Y LOS EPDPEI PARA LA INTEGRACIÓN Y ARMONIZACIÓN DE REGÍMENES NORMATIVOS

El objetivo primario del RGPD es la armonización del nivel de protección en los veintiocho Estados miembros de la Unión Europea, especialmente a raíz de la heterogeneidad de marcos nacionales reguladores de la protección de datos, consecuencia de la flexibilidad dejada por la Directiva 95/46/CE a los Estados en su transposición, de ahí el instrumento normativo elegido: un Reglamento, de aplicación directa en los Estados miembros, que sustituye a la anterior Directiva. Hay una decidida voluntad, no ya de aproximar las legislaciones nacionales, sino de instaurar un régimen uniforme que contribuya efectivamente a la integración económica y social en el mercado único digital de la Unión Europea. Como se indicado, en materia de protección de datos, Europa pasa a regirse por el axioma «un continente, una norma»[19].

[19] .- Ciertamente, el RGPD contiene algunas remisiones a las normas internas, de manera que los Estados conservan aún ciertas posibilidades de actuación, aunque sean limitadas (así, por ejemplo, lo previsto en el artículo 8 en relación con la edad mínima para consentir lícitamente en el marco de la prestación de servicios de la Sociedad de la Información; la posibilidad otorgada a loa Estados, por el artículo 9.4, en relación con los datos genéticos, datos biométricos y datos relativos a la salud, de mantener o introducir condiciones adicionales o, incluso, limitaciones; o el establecimiento, conforme al artículo 85, de normas para la conciliación de la libertad de expresión y la protección de datos) y ofrece a los Estados miembros la posibilidad de precisar aún más la aplicación de las normas de protección de datos en sectores específicos como: sector público (art. 6.2), empleo y seguridad social (art. 9.2.b y 88), medicina preventiva y medicina laboral, sanidad pública (art. 9.2.h. e i), archivo con fines de interés público, investigación científica o histórica o con fines estadísticos (art. 9.2.j y 89), acceso público a los

Pero a este primer objetivo se suma otro más ambicioso, ser referente mundial y extender el estándar europeo de protección de datos a otras áreas geográfico-económicas[20], favoreciendo los flujos internacionales de datos en un mercado digital, en continua evolución y basado en la ubicuidad que proporciona internet, con el consiguiente desvanecimiento de los límites territoriales de legalidad y jurisdicción. Esto se trata de alcanzar con algunas medidas:

1.- Ampliando el ámbito de aplicación territorial de la legislación europea en materia de protección de datos personales. El RGPD es de aplicación, no sólo a responsables y encargados de tratamiento establecidos en la Unión Europea, sino también a operadores radicados fuera de la Unión que ofrezcan servicios o bienes a interesados que, según la versión oficial del RGPD en español, residan en la Unión o controlen su comportamiento en territorio de la misma. No obstante el pasado 19 de abril de 2018 se publicó un documento del Consejo Europeo que, amparado en el procedimiento de corrección de errores materiales y de traducción, introduce modificaciones al texto de diversos considerandos y varios artículos del RGPD. Probablemente la corrección más relevante y la vez más significativa sea la del art. 3.2 RGPD y sus correlativos considerandos 23, 24 y 80, dado que, suprimiendo el concepto de "residencia" y los problemas interpretativos a que podía conducir, amplía el ámbito de aplicación territorial del RGPD afectando, no ya a los tratamientos de datos de las personas "residentes" en la Unión Europea, sino a los de las personas "que se encuentren" en la Unión Europea. Este alcance territorial del RGPD, sin duda, obliga a agentes internacionales y prestadores de servicios tecnológicos que operan a escala mundial a adaptarse a la normativa europea de protección de datos.

Además el nuevo enfoque delimitador del ámbito de aplicación, centrado en las personas en cuanto destinatarias de los servicios o cuyo comportamiento es objeto de control, se ve asimismo favorecido por la introducción de un sistema de "ventanilla única" o "*one-Stop-shop solution*", que implica para los titulares de los datos hacer valer sus derechos con facilidad ante su autoridad nacional de protección de datos, aun cuando sus datos se traten fuera de su país de origen.

---

documentos oficiales (art. 86), número nacional de identificación (art. 87), y obligaciones de secreto (art. 90).

Algunos Estados europeos (Alemania, Austria, Francia) han aprobado ya normas nacionales de adaptación. En España, a fecha de elaboración de este trabajo -junio 2018-, se encuentra en tramitación en el Congreso de los Diputados (en fase de negociación en la Comisión de Justicia de las 369 enmiendas presentadas), el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (Boletín Oficial del Congreso de los Diputados, de 24 de noviembre, núm. 13-1; PLOPD, en lo sucesivo), que adaptará la Ley Orgánica anterior (15/1999, de 13 de diciembre) al nuevo marco normativo establecido en la Unión Europea.

[20] .- Esta pretensión se ha hecho efectiva en la negociación del Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 108). El convenio modernizado aumenta considerablemente el grado de protección de datos con arreglo al Convenio 108 y recoge un planteamiento y principios idénticos al nuevo estandar de protección de datos europeo derivado del RGPD. El pasado 5 de junio de 2018, la Comisión Europea publicaba la Propuesta de Decisión del Consejo por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo modificativo [Bruselas, 5.6.2018 COM(2018) 451 final].

Igualmente, las empresas sólo tendrán que acudir a la autoridad competente del país en el que tengan su sede central, lo que simplificará y abaratará operar en toda la Unión Europea. El punto de partida será determinar la autoridad de control competente en materia de reclamaciones, sanciones o supervisión cuando se esté ante un "tratamiento transfronterizo" intracomunitario, lo que engloba dos situaciones conforme a la definición contenida en el artículo 4.23 RGPD:

a. El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o
b. El tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

En tal caso, corresponde a la autoridad de control del establecimiento principal o único del responsable o encargado la consideración de autoridad de control principal, debiendo actuar conforme al procedimiento de cooperación previsto en el artículo 60 RGPD con las demás autoridades de control interesadas (por ejemplo, por resultar afectados quienes se encuentren en ese Estado, por haberse presentado una reclamación ante esa autoridad, por tratarse de un tratamiento realizado por un responsable o encargado establecido en el Estado miembro de esa autoridad…). Esta cooperación se basa, por una parte, en la asistencia mutua, a fin de aplicar el presente Reglamento de manera coherente (artículo 61), y en la posibilidad de que realicen operaciones conjuntas en investigaciones o para hacer un seguimiento de la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro (artículo 62). Junto con estas medidas se contempla el denominado mecanismo de coherencia (artículo 63), quedando el Comité Europeo de Protección de Datos como garante de la aplicación de soluciones uniformes, resolviendo de forma vinculante cuando haya conflicto entre varias Autoridades implicadas.

2. Otros instrumentos, dirigidos a promover un marco global de aseguramiento transversal y transfronterizo de los principios jurídicos europeos de protección de datos, vienen de la mano del fomento de estándares internacionales del tratamiento de datos personales, a través del impulso de medidas tendentes a la autorregulación, como los Códigos tipo o las Normas corporativas vinculantes *(Binding Corporate Rules, BCRs),* que suponen sistemas internos de control eficaz en tanto que parten de los propios responsables y encargados de los tratamientos de datos y aportan un valor añadido en cuanto que complementan o especifican la aplicación de la normativa general al concreto sector o ámbito.

a. Las normas corporativas vinculantes son normas adoptadas en el seno de corporaciones multinacionales con sucursales y filiales en países dentro y fuera de la Unión Europea, con el objetivo de flexibilizar los flujos de datos entre las diferentes sedes del grupo. Aparecen definidas en el artículo 4 del Reglamento como «las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de

un Estado miembro de la Unión para las transferencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo de empresas o grupo de sociedades que participen en una actividad económica conjunta». Son objeto de regulación detallada en el artículo 47, que establece la necesidad de que se apliquen y cumplan internamente por todos los miembros del grupo de empresas o grupo de sociedades, siendo jurídicamente vinculantes también a nivel externo, así como que confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales.

b. Además del reconocimiento expreso de la validez de las normas corporativas vinculantes en relación con las transferencias internacionales de datos (no exigiéndose la tradicional autorización por parte de la autoridad de control competente), se reconoce la posibilidad de otorgar validez general dentro de la Unión Europea a los códigos de conducta sometidos a examen de la Comisión que, al tiempo de servir como mecanismo de verificación del cumplimiento de determinadas obligaciones impuestas por la normativa, podrán constituir garantía adecuada en el marco de las transferencias internacionales de datos ofrecida por responsables o encargados de tratamiento de terceros países, a los que no se aplica el RGPD, que se adhieran a ellos. Los Códigos, conforme a lo dispuesto por el artículo 40 del Reglamento, serán promovidos por los Estados Miembros, las autoridades de control, el Comité Europeo de Protección de Datos y la Comisión, atendiendo a las peculiaridades de cada sector y de las pequeñas y medianas empresas. Si el tratamiento objeto del código afecta a un solo Estado Miembro, 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 Comité 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.

Los EPDPEI se valen igualmente de algunas de estas herramientas implementadas por el RGPD para alcanzar sus objetivos de armonización y homogeneización:

1. En línea con los nuevos supuestos de aplicación que introduce el RGPD, el ámbito de aplicación territorial de los EPDPEI se extiende, no sólo a los responsables o encargados establecidos en territorio de los Estados Iberoamericanos (art. 5.1.a), sino también a operadores no establecidos que dirijan ofertas de bienes o servicios a residentes en los Estados Iberoamericanos o realicen actividades de tratamiento relacionadas con el control de su comportamiento (art. 5.1.b). Además recoge como punto de conexión un criterio presente en el art. 4.1.c de la derogada Directiva 95/46/CE, el "recurso a medios situados en el territorio de dicho Estado miembro", así se establece que los EPDPEI serán aplicables a un responsable o encargado no establecido que utilice o recurra a medios, automatizados o no, situados en territorio de los Estados Iberoamericanos, salvo que dichos medios se utilicen solamente con fines de tránsito (art. 5.1.d); criterio que ha quedado englobado en el RGPD en el cambio de enfoque centrado en la persona cuyos datos se tratan ("personas que se encuentren en la Unión Europea").

2. Del mismo modo, los EPDPEI fomentan los mecanismos de autorregulación a los que un responsable puede adherirse de forma voluntaria que serán validados o reconocidos conforme a las reglas establecidas por cada legislación nacional y el desarrollo de códigos deontológicos y sistemas de certificación (art. 40).

III. CLAVES DE LA CONVERGENCIA ENTRE SISTEMAS

Varios son los ejes que ponen de relieve la influencia del RGPD en los EPDPEI, y contribuirán a la convergencia entre el sistema jurídico europeo y aquellos países iberoamericanos que implementen los Estándares.

1. LOS PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

En materia de principios, el RGPD refuerza y amplia los tradicionales recogidos en la Directiva 46/95/CE, que distinguía entre los relativos a la calidad (art. 6) y los relativos a la legitimación (art. 7). El artículo 5 del RGPD establece que los tratamientos de datos de carácter personal deberán ajustarse a una serie de principios que coinciden con los previstos en el artículo 10 EPDPEI, desarrollados en preceptos posteriores.

No obstante, hay un matiz diferencial. Tanto RGPD como EPDPEI refieren los tratamientos incluidos bajos su ámbito de aplicación a los relativos a datos de personas físicas, identificadas o identificables, quedando excluidos los concernientes a la información de las personas jurídicas o a los datos de las personas fallecidas. No obstante, mientras que el RGPD (considerando 27) excluye claramente los datos de personas jurídicas y deja la puerta abierta para que los Estados miembros establezcan normas específicas relativas al tratamiento de datos de las personas fallecidas[21], los

[21] .- En el PLOPD español se incluye la posibilidad de que los herederos ejerciten derechos en nombre del fallecido, pudiendo solicitar la supresión o cancelación. En concreto, el artículo 3 PLOPD indica que los herederos podrán dirigirse al responsable del tratamiento de los datos, excepto si la persona fallecida «lo hubiese prohibido expresamente o así lo establezca la ley». Igualmente, también podrán acceder a los datos «el albacea testamentario, así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello». Los requisitos y condiciones para acreditar la validez de este mandato estarán recogidos en un Real Decreto que tendrá que aprobarse posteriormente. En caso de los menores, la propuesta legislativa establece que esta decisión estará en manos de sus representantes legales o, en el marco de sus competencias, del Ministerio Fiscal. Una situación similar sucederá con el fallecimiento de las personas discapacitadas, con el añadido de que también podrán solicitar la rectificación y supresión de los datos «quienes hubieran sido designados para el ejercicio de funciones de apoyo». Asimismo, la Disposición adicional séptima PLOPD prevé la aplicación de las mismas reglas en cuanto el acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información a favor de personas que hayan fallecido, a saber: "a) *Los herederos de la persona fallecida podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión. Como excepción, los herederos no podrán acceder a los contenidos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones. c) En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona*

EPDPEI permiten, no solo que la legislación nacional de los Estados iberoamericanos pueda reconocer a las personas físicas vinculadas a fallecidos o designados por estos ejercitar derechos en relación con los datos personales de fallecidos (art. 32.3), sino también disponer que la "*información de las personas jurídicas sea salvaguardada acorde con el derecho a la protección de datos personales*" (art. 4.2).

Con esta precisión, se analiza, a continuación, la correspondencia entre los principios aplicables al tratamiento de datos personales en ambos textos, siguiendo la enunciación realizada por el legislador europeo.

1.1. **Licitud, lealtad y transparencia en relación con el interesado**.

La licitud requiere que los tratamientos se basen en alguna de las condiciones previstas en el artículo 6 RGPD, a saber: a) el consentimiento del interesado; b) la necesidad del tratamiento para la ejecución de un contrato o para la aplicación a petición de este de medidas precontractuales; c) cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) protección de intereses vitales del interesado o de otra persona física; e) cumplimiento de una misión realizada en interés público o ejercicio de poderes públicos conferidos al responsable del tratamiento; f) satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Tales bases están recogidas en el artículo 11 de los EPDPEI, bajo la rúbrica principio de legitimación, que aclara dos supuestos más: la necesidad del tratamiento para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente (11.1.b.) y para el reconocimiento o defensa de los derechos del titular ante una autoridad pública (11.1.d.)

La lealtad, sólo mencionada en el RGPD, es desarrollada por el artículo 15 EPDPEI que advierte que "*el responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos*", considerando desleales aquellos tratamientos "*que den lugar a una discriminación injusta o arbitraria contra los titulares*".

La transparencia es un concepto nuevo y clave en el RGPD; como se advierte en el considerando 39, «exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de

---

física o jurídica interesada. d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los citados mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta Ley Orgánica".

los datos personales que les conciernan que sean objeto de tratamiento» Dos son, pues, los principales aspectos de la transparencia que debe estar presente en todo el proceso de tratamiento de los datos: uno, a iniciativa del responsable: la información que debe facilitarse al interesado (notablemente ampliada por el regulador europeo conforme a las previsiones de los artículos 13 y 14 RGPD); y otro, a iniciativa del titular de los datos, el derecho a conocer si se están tratando sus datos y, en tal caso, obtener información del responsable sobre el tratamiento (sus fines, categorías de datos tratados, destinatarios, plazo de conservación…) en los términos del artículo 15 RGPD. Ambos aspectos aparecen reflejados, aunque no de manera tan amplia como en la norma europea, en los artículos 16 (principio de transparencia) y 25 (derecho de acceso) de los EPDPEI.

1.2. Limitación de la finalidad

Este principio, con esta denominación en el RGPD y en el artículo 17 EPDPEI bajo la rúbrica "principio de finalidad", aparece en ambos textos en los mismos términos: los datos personales solo serán recogidos para fines determinados, explícitos y legítimos, garantizando que no serán tratados ulteriormente de manera incompatible con dichos fines, si bien el tratamiento posterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales, pudiendo llevarse a cabo por el responsable);

1.3. Minimización, exactitud y limitación del plazo de conservación

Estos tres principios recogidos en el artículo 5.1.c, d, y e RGPD encuentran su reflejo en el artículo 19 EPDPEI, que los engloba bajo la rúbrica "principio de calidad", al igual que ya lo hiciera la Directiva 46/95/CE de los datos. Su cumplimiento exige que los datos:

- Sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Es el conocido principio de minimización que, al limitar la cantidad de datos personales recopilados o retenidos, comporta una significativa reducción del riesgo de su vulneración y de uso para finalidades diferentes de aquellas para las que se recabaron.
- Exactos y, si fuera necesario, actualizados;
- Conservados "*durante no más tiempo del necesario para los fines del tratamiento de los datos personales".*

1.4. Integridad y confidencialidad

Estos nuevos principios en el RGPD se corresponden con el principio de seguridad del artículo 21 EPDPEI y el de confidencialidad del artículo 23 EPDPEI, e imponen la protección contra el tratamiento no autorizado o ilícito de datos y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.

1.5. Responsabilidad proactiva

Este nuevo principio introducido por el legislador europeo impregna todo el articulado del RGPD: el responsable del tratamiento debe implementar medidas apropiadas de garantía y cumplimiento de los principios y obligaciones en materia de protección de datos, que minimicen los riesgos derivados de una mala práctica, debiendo establecer mecanismos dirigidos a evaluar su fiabilidad (auditorías internas y externas) y poder demostrar su efectividad; debe garantizar los principios relativos al tratamiento y ser capaz de demostrarlo. Los EPDPEI lo consagran en el artículo 20, cuyo apartado 3, enumera, a título enunciativo, algunos de los mecanismos que el responsable podrá adoptar para su cumplimiento:

a. *Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.*
b. *Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.*
c. *Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.*
d. *Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.*
e. *Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.*
f. *Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.*
g. *Establecer procedimientos para recibir y responder dudas y quejas de los titulares.*

2. MAYOR CONTROL SOBRE LOS PROPIOS DATOS

Desde la perspectiva de las personas, titulares de los datos, el RGPD ofrece una mayor protección y otorga una mayor control sobre el manejo y utilización de sus datos por los operadores, básicamente a través de dos mecanismos: exigiendo un consentimiento de más calidad cuando la licitud del tratamiento encuentra su base en él y ampliando el catálogo de derechos del interesado. Ambos aspectos aparecen reflejados, con algún matiz diferencial, en los EPDPEI.

2.1. Consentimiento de más calidad

Ambos textos definen el consentimiento como una manifestación de voluntad por la que el interesado acepta, a través de una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen, caracterizada por cuatro cualidades: libre, específica, informada e inequívoca (arts. 4.11 RGPD y 2.1.b EPDPEI). Consentimiento, además, verificable, (recayendo la carga de su prueba en el responsable del tratamiento) y revocable (arts. 12 EPDPEI).

Son numerosas las novedades respecto del concepto de consentimiento en el RGPD. A la luz del documento "Directrices sobre el consentimiento conforme al Reglamento

2016/679", cuya versión final ha sido adoptada el pasado 10 de abril de 2018 (Documento WP 259rev.01)[22], elaboradas por el Grupo de Trabajo del Artículo 29 (en adelante GT29)[23], la validez del consentimiento requiere que sea:

a. Libre, esto es, debe prestarse conscientemente y sin influencias indebidas (vicios del consentimiento, engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta) que induzcan la elección del titular de los datos en un determinado sentido. Si las consecuencias del consentimiento socavan la libertad de elección de la persona, el consentimiento no es libre. El artículo 7 del RGPD incide en este atributo de dos formas:

- Por una parte, indicado en su apartado 2 que, si el consentimiento del interesado se ha de dar en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento deberá presentarse de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo; aspectos estos últimos de accesibilidad y calidad de la presentación que entroncan con el principio de transparencia de la información (art. 12 RGPD). Habrá, pues, falta de libertad cuando no se permita dar consentimiento por separado a las distintas operaciones de tratamiento de datos pese a ser lo adecuado en ese caso concreto (considerando 43 RGPD).
- Por otra parte, al señalar, en su apartado 4, que para evaluar si el consentimiento se ha otorgado libremente se tendrá en cuenta el hecho de que la ejecución de un contrato, o la prestación de un servicio, se haya condicionado a la autorización de un tratamiento de datos que no sea necesario para el cumplimiento del mencionado contrato. El considerando 43 RGPD, recogiendo esta idea, va más allá al precisar que, para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido en un caso particular cuando exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando el responsable es una autoridad pública y es poco probable que el consentimiento se haya dado libremente en todas las circunstancias de esa situación específica.

El GT29 clarifica estas dos relevantes cuestiones relativas al desequilibrio de poder entre el responsable del tratamiento y el titular de los datos personales y a la condicionalidad del consentimiento, en el sentido de que debe prestarse especial atención al hecho de que el consentimiento esté «agrupado» (*bundling*) con la aceptación de términos y condiciones o «atado» a la provisión de un contrato o un servicio cuando los datos personales solicitados no son necesarios para el cumplimiento del contrato o la prestación de servicio. El consentimiento libre significa que no esté sometido a condición alguna. Además recoge otro elemento: el p*erjuicio:* lo que significa que el responsable del tratamiento tiene que demostrar tanto que el interesado «goza de verdadera o libre elección» a la hora de dar su consentimiento, como que puede denegar o retirar o revocar su consentimiento «sin sufrir perjuicio alguno (considerando 42 RGPD)

[22].- Accesible en http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[23] .- El GT29, hasta el 25 de mayo de 2018, reunía a las autoridades de protección de datos de todos los Estados miembros de la Unión Europea y, desde esa fecha, ha sido sustituido por el Comité Europeo de Protección de Datos (CEPD).

b. Específico, lo que supone la concreción de los fines, que deben ser explícitos y legítimos, para los que se recaban los datos, sin que puedan ser tratados posteriormente de manera incompatible con dichos fines (principio de especificidad o limitación de los fines). Debe tratarse de un consentimiento «granularizado».

La granularidad hace referencia al consentimiento diferenciado por cada finalidad de tratamiento de datos (v.gr., consentimiento para actividades de marketing directo y consentimiento para compartir datos con terceros). No serán admisibles cláusulas en las que el titular de los datos se ve forzado a consentir en bloque múltiples finalidades del tratamiento sin posibilidad real de aceptar unas y rechazar otras[24].

c. Informado, lo que supone la exigencia de que, antes de la emisión del consentimiento, se cuente con información exacta y completa sobre la identidad del responsable, los fines del tratamiento, el plazo de conservación de los datos…; cualidad del consentimiento que no es más que aplicación de los principios de lealtad y transparencia[25].

d. Consentimiento inequívoco. El Reglamento sigue en este aspecto las previsiones del artículo 7 de la Directiva 95/46/CE aunque, frente a las diferentes interpretaciones que los Estados miembros habían hecho del término "inequívoco", se decanta por exigir una declaración o una clara acción afirmativa. Lo que añade el RGPD es que el interesado acepte el tratamiento de sus datos personales a través de una declaración, que puede ser

[24] .- La falta de vinculación del consentimiento a finalidades específicas y de información, y por tanto de un consentimiento válido, ha motivado una reciente sanción de la AEPD por la comunicación de datos realizada por Whatsapp a Facebook. Una denuncia formulada respecto a los términos de servicio que Whatsapp introdujo en agosto de 2016 para obtener el consentimiento de sus usuarios para ceder sus datos personales a Facebook, que la había adquirido. Este consentimiento se otorgaba mediante una casilla marcada por defecto (lo cual en aquel momento tenía base normativa, al admitirse el consentimiento tácito en España) ligada a una pestaña de visualización opcional. La finalidad de recogida en el texto que acompañaba la casilla era: "*Compartir la información de mi cuenta de Whatsapp con Facebook para mejorar mi experiencia con los productos y publicidad en Facebook. Tus chats y número telefónico no serán compartidos en Facebook*". En marzo de 2018, la autoridad de control española, AEPD, ha dado por probadas dos infracciones graves de la Ley Orgánica de Protección de Datos española y multado a cada una de las empresas con 300.000 euros, la cuantía máxima correspondiente a las infracciones graves declaradas: una de ellas directamente a la aplicación de mensajería instantánea por «comunicar datos a Facebook sin haber obtenido un consentimiento válido de los usuarios» y otra a la empresa matriz «por tratar esos datos para sus propios fines sin consentimiento». La resolución añade que la información sobre a quién se pueden ceder los datos, las finalidades para las que se le ceden o la utilización que harán de los mismos los cesionarios «se ofrece de forma poco clara, con expresiones imprecisas e inconcretas que no permiten deducir, sin duda o equivocación, la finalidad para la cual van a ser cedidos»

También la ausencia de consentimiento está también detrás de la sanción de 300.000 euros impuesta, el pasado 7 de noviembre de 2017, a Google por la AEPD, en relación con su servicio *Street View* por una infracción grave al constatar que recogió y almacenó datos personales transmitidos a través de redes WiFi abiertas, sin que los afectados tuviesen conocimiento de dicha recogida y sin el consentimiento de los mismos.

[25] .- En España, el PLOPD (art. 11), en tramitación parlamentaria, establece la posibilidad de que la información a los interesados se facilite por capas, proporcionando, en un primer nivel, la información esencial sobre las principales circunstancias del tratamiento de datos y, en un segundo nivel, la información extensa que complementa la de carácter básico.

por escrito, inclusive por medios electrónicos, o verbal, o que se dé mediante un acto afirmativo claro, poniendo fin de esta manera a la posibilidad de tratar datos personales sobre la base del consentimiento tácito.

Al respecto, el GT29 deja claro que las casillas pre-marcadas, el silencio o la inactividad del interesado o el simple hecho de proceder con el uso de un servicio, incluir el consentimiento como parte de los términos y condiciones generales o el uso de casillas opto ut (de exclusión voluntaria), no puede ser considerado como una indicación activa de elección y que tampoco puede obtenerse por el hecho de acordar un contrato o de aceptar los términos y condiciones aplicables a un servicio.

RGPD y EPDPEI dedican especial atención al tratamiento de datos personales de menores y su capacidad para emitir el consentimiento. El RGPD reconoce, en relación con la oferta directa de servicios de la sociedad de la información a menores, la licitud del consentimiento emitido por los mayores de 16 años, o incluso por menores a esta edad, siempre que no sea inferior a 13 años, si lo permite la legislación nacional de un Estado miembro. En otro caso, solo será lícito si el consentimiento ha sido dado o autorizado por el titular de la patria potestad o tutela (art. 8). Los EPDPEI parten de que en caso de menores el tratamiento debe ser autorizado por titular de la patria potestad o tutela, salvo que la legislación interna de cada Estado iberoamericano haya establecido una edad mínima (art. 13). Ambos textos añaden que «el responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño o por el propio menor, teniendo en cuenta la tecnología disponible»

El RGPD añade un *plus* al consentimiento cuando va referido:

a. al tratamiento de categorías especiales de datos personales (art. 9). Son datos que el Reglamento les otorga una especial protección, ya sea por su naturaleza o por la relación que puedan tener con los derechos y las libertades fundamentales de las personas: origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, con el objetivo de identificar de manera exclusiva a un individuo, datos relativos a la salud o la vida sexual y/o la orientación sexual.
b. a las decisiones basadas únicamente en el tratamiento automatizado de datos personales, incluida la elaboración de perfiles (art. 22.1.c) y
c. a la transferencia internacional de datos a terceros países u organizaciones internacionales cuando no haya nivel adecuado de protección (art. 49).

En estos casos se exige que sea "explícito". El GT29, en sus directrices, distingue entre el consentimiento normal, al que se refiere como *«regular consent»*, y el consentimiento explícito, aclarando que este último es exigible cuando hay un alto riesgo para la protección de los datos personales y, por tanto, es necesario un alto nivel de control del interesado sobre sus datos personales.

Como para el *«regular consent»* el RGPD exige una "clara acción afirmativa", para el consentimiento explícito se requiere un estándar más alto para su obtención. Esto puede incluir la provisión expresa de consentimiento en una declaración escrita firmada por el individuo. También puede incluir completar un formulario electrónico, enviar un correo electrónico, cargar un documento escaneado firmado, usar una firma electrónica, una

confirmación presionando un botón, tecla o una casilla de verificación, un sistema de doble verificación a través del envío y *click* de un enlace por correo o de un código por SMS para confirmar el acuerdo…

Los EPDPEI circunscriben la exigencia de un consentimiento "expreso y por escrito" a los datos personales de carácter sensible (art. 9).

2.2. Nuevos y reforzados derechos ARCO

En esta misma línea de otorgar a la persona un mayor control sobre sus datos, el RGPD refuerza los tradicionales derechos ARCO (acceso, rectificación, cancelación y oposición) e incorpora otros nuevos. Se añaden los de limitación del tratamiento, portabilidad, oposición a decisiones automatizadas y comunicación al interesado sin dilación indebida de las violaciones de seguridad que entrañen un alto riesgo para los derechos y libertades de las personas físicas. Estos mismos derechos se encuentran reconocidos en los EPDPEI

Por lo que se refiere a los tradicionales derechos ARCO:

a. El derecho de acceso (arts. 15 RGPD y 25 EPDPEI), que permite al titular de los datos obtener información sobre sus datos personales sometidos a tratamiento. La nueva normativa europea amplia, respecto de la Directiva 95/46/CE, el contenido de la respuesta que debe ofrecer el responsable del tratamiento, incorporándose aspectos como el plazo de conservación de los datos, las transferencias internacionales, la posibilidad de reclamar ante la autoridad de control, tratamiento automatizados que incluyan la elaboración de perfiles…

b. El derecho de rectificación de los datos inexactos es objeto de previsión específica en los artículos 16 RGPD y 26 EPDPEI. El RGPD, además, atribuye un derecho nuevo al interesado, el derecho a completar el tratamiento, esto es, la capacidad de exigir del responsable del tratamiento que complete los datos sometidos a tratamiento con información adicional, es decir que se añada al tratamiento de los datos la información que interese aportar al interesado.

c. El derecho de supresión, conforme al artículo 17 RGPD, concede al interesado la posibilidad a exigir del responsable que excluya del tratamiento los datos de carácter personal que resulten innecesarios para el fin que justificó el tratamiento, por no interesarle que se sometan a tratamiento, porque el tratamiento infrinja los principios en materia de protección de datos, o por imperativo legal. Se reconoce también en el artículo 27 EPDPEI.

d. El derecho de oposición es regulado en términos prácticamente coincidentes en los artículos 21 RGPD y 28 EPDPEI, que hacen mención expresa al tratamiento con fines de mercadotecnia directa como supuesto que legitima en todo caso la oposición del interesado. Se trata de un derecho que resulta ampliado con las previsiones relativas al nuevo derecho a oponerse a ser objeto de una decisión individual automatizada, incluida la elaboración de perfiles, recogido por los artículos 22 RGPD y 29 EPDPEI.

e. A tales derechos cabe añadir el derecho a ser indemnizado de los daños y perjuicios materiales o inmateriales sufridos como consecuencia de una infracción de los principios en materia de protección de datos (arts. 23 RGPD y 44 EPDPEI).

Como nuevos derechos que fortalecen el poder de disposición del titular sobre sus datos, se contemplan:

1. El derecho a la portabilidad, consistente en la posibilidad que tiene el titular de los datos personales por un lado de obtener una copia de dichos datos en un formato electrónico comúnmente utilizado, de lectura mecánica; y, por otro lado, la posibilidad transferir dichos datos si la tecnología lo permite a otros proveedores de servicios sin que lo impida el responsable al que se los hubiera facilitado (arts. 20.1 RGPD y 30 EPDPEI). Esto es, se trata de obtener una copia susceptible de ser procesada sin dificultad (lectura mecánica) con el fin de garantizar la interoperabilidad de los datos en un entorno digital, mientras que el acceso se limita a garantizar la información en sí misma susceptible de lectura humana. La portabilidad, según las Directrices elaboradas por el GT29 sobre el derecho a la portabilidad de los datos, cuya versión final fue adoptada el pasado 5 de abril 2017 (Documento WP 242rev.01) [26], se extiende solo a los datos personales proporcionados o facilitados por el titular (nombre y apellidos, domicilio, etc.) y a aquellos derivados del servicio disfrutado por el titular (consumos, historial de búsqueda, datos de localización, etc.). Un alcance algo más amplio parece conceder a este derecho el artículo 30.1 EPDPEI en tanto que lo extiende no sólo a *"datos personales que hubiere proporcionado al responsable"* sino también, con carácter disyuntivo, a los *"que sean objeto de tratamiento*". Si bien respecto de información deducida de los datos y generada por el propio responsable del tratamiento, el artículo 30.4 EPDPEI contiene una previsión aclaratoria que no recoge el RGPD: "*Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles*". Es este un aspecto que diferencia el derecho de acceso, que incluye datos personales e información deducida de los mismos, y el derecho de portabilidad, limitado a los datos personales.

2. Derecho a la limitación-restricción del tratamiento (art. 18 RGPD y 31 EPDPEI). El interesado tendrá derecho a obtener del responsable la limitación del tratamiento de sus datos personales, según la normativa europea, cuando: a) impugne la exactitud de los datos, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los mismos; b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar a limitación de su uso; c) el responsable del

[26] .- El GT29, en sus Directrices sobre el derecho a la portabilidad, aclara, además, que el derecho a la portabilidad de los datos no es un derecho general, sólo será aplicable cuando exista: a. un tratamiento automatizado de datos personales y b. basado en el consentimiento del titular o en la existencia de una relación contractual. Y a efectos de favorecerlo, advierte que una práctica recomendable es que los responsables del tratamiento comiencen a desarrollar los medios que contribuyan a responder a las solicitudes de portabilidad de datos, como herramientas de descarga o Interfaces de Programación de Aplicaciones (APIs). Además cuando entre los datos recuperados y transmitidos existan datos personales de terceros se requiere que la portabilidad no afecte negativamente a sus derechos y libertades. En este sentido se indica en el documento: «Por ejemplo, un servicio de correo web puede permitir al interesado la creación de un listado de sus contactos, amigos, parientes, familiares y entorno social en general. Puesto que estos datos se refieren a la persona física identificable que desea ejercer su derecho a la portabilidad de los datos (y han sido creados por ella), los responsables del tratamiento deben transmitir al interesado la totalidad del listado de correos electrónicos entrantes y salientes….Y a la inversa, los derechos y libertades de los terceros no se respetarán si el nuevo responsable del tratamiento utiliza los datos personales para otros fines, por ejemplo, si el responsable receptor utiliza los datos personales de otras personas que figuran en el listado de contactos del interesado con fines de mercadotecnia». Puede consultarse el documento en https://www.aepd.es/media/criterios/wp242rev01-es.pdf

tratamiento ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; o d) el interesado se ha opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable del tratamiento prevalecen sobre los del interesado. Tales supuestos son coincidentes con las previsiones del art. 31 EPDPEI. Se trata del marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro (art. 4.3 RGPD) incrustando alguna señal o distintivo que impida su tratamiento. Como señala el considerando 67 RGPD: "Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet".

3. Derecho a no ser objeto de elaboración de perfiles (arts. 22 RGPD y 29 EPDPEI)[27]. Se trata una facultad relacionada con las técnicas automatizadas de procesamiento y análisis masivo de datos (*big data*), en concreto, el art. 4.4 RGPD define la elaboración de perfiles como "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física"*.

Esta nueva facultad parte de prohibir la toma de decisiones individualizadas totalmente automáticas, incluida la elaboración de perfiles, que tenga efectos jurídicos en el interesado o le afecte significativamente de modo similar. Es decir, una decisión basada únicamente en el tratamiento automatizado sin participación humana alguna en el proceso de toma de la decisión. Tal prohibición tiene tres excepciones:

- cuando la toma de decisiones automática es necesaria celebración o la ejecución de un contrato.
- cuando esté autorizada por ley europea o de un Estado miembro (por ejemplo, la legislación contra la evasión de impuestos), según el RGPD, o por el derecho interno de los Estados iberoamericanos conforme a los EPDPEI, y
- cuando los interesados han dado su consentimiento explícito, según el RGPD, o consentimiento demostrable, conforme a los EPDPEI.

Salvo cuando este tipo de toma de decisiones se base en una ley, en los otros dos casos los responsables deberán informar a la persona[28], como mínimo, de lo siguiente:

---

[27] .- Directrices del GT29 sobre decisiones individuales automatizadas y perfilado a los efectos del Reglamento (UE) 2016/679 (WP 251rev01), cuya versión final ha sido adoptada el 6 de febrero de 2018, accesible en http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[28] .- Este deber de información constituye una vertiente más del principio de transparencia en los tratamiento de datos que puede revestir serias dificultades en procesos basados en *big data* en los que interviene la inteligencia artificial y sistemas de aprendizaje profundo, en los que los resultados de los algoritmos aplicados son imprevisibles y sólo se conocen al final, así como colisionar con derechos de propiedad intelectual, secretos comerciales o comportar riesgos para la seguridad en defensa, vid. LÓPEZ CALVO, J., "Inteligencia Artificial y derecho de «explicación» en el Reglamento Europeo de Protección de Datos", *Diario La Ley*, n.º 16, Sección Ciberderecho, 10 abril 2018.

— La lógica aplicada en el proceso de toma de decisiones.
— El derecho que poseen a obtener intervención humana.
— Las posibles consecuencias del tratamiento.
— El derecho a impugnar la decisión que les corresponde.

4. Derecho a ser informado de cualquier brecha de seguridad que pueda suponer un alto grado de riesgo para sus derechos y libertades de las personas, por ejemplo problemas de discriminación, usurpación de identidad o fraude, pérdidas económicas, menoscabo de la reputación, cambio no autorizado de la seudonimización, pérdida de confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social significativo. El responsable del tratamiento comunicará al interesado, sin demora injustificada, la violación de datos personales (arts. 32 RGPD y 22 EPDPEI). También se impone al responsable la obligación de informar a la Autoridad de Protección de Datos competente sobre las posibles brechas de seguridad que se hubieran producido en relación con los tratamientos de datos personales que lleve a cabo. Esta notificación deberá realizarse a la Autoridad de Control, según la norma europea, en un plazo máximo de 72 horas desde que se tiene constancia de que la brecha se ha producido.

5. Especial mención requiere el denominado «derecho al olvido» (art. 17 RGPD), centrado en la protección de la persona respecto de la información publicada en internet y que, con independencia de su origen y de si es verdadera o no, podría afectar a su desarrollo ulterior como personas. Llama la atención este nuevo derecho no haya sido recogido en los EPDPEI.

En la normativa europea, es un nuevo derecho que se plantea como una extensión del derecho de supresión en el entorno digital, ya que sólo procede en aquellos casos en que aplica el derecho de supresión, es decir, cuando se solicita la cancelación de los datos por las siguientes razones:

- Los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados.
- El interesado retira el consentimiento en que se basa el tratamiento, o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos.
- El interesado se opone al tratamiento de datos personales por motivos relacionados con su situación particular respecto de tratamientos basados en el cumplimiento de una misión de interés público o satisfacción de intereses legítimos del responsable o terceros, salvo que el responsable del tratamiento acredite motivos imperiosos y legítimos que prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado.
- Cuando los datos personales hayan sido tratados ilícitamente.
- Cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

En tales casos el responsable del tratamiento de los datos asume la obligación de suprimir los datos personales identificados en la reclamación «sin dilación», así como la obligación de informar a los responsables que estén tratando tales datos de la solicitud del interesado, a efectos de que se suprima cualquier enlace a esos datos, o cualquier copia o réplica de estos.

Como se advierte en el considerando 65 RGPD, es un derecho especialmente "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".

No obstante, se establecen una serie de excepciones a los derechos de supresión y al olvido basadas en el ejercicio de la libertad de expresión e información, cumplimiento de una obligación legal o de una misión realizada en interés público, en razones de interés público en el ámbito de la salud pública, fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o el ejercicio o la defensa frente a reclamaciones.

Un antecedente de la regulación del derecho al olvido en el RGPD lo constituye la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 13 de mayo de 2014 en el asunto C-131/12 (el «Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González»), si bien la concepción del derecho al olvido que resulta de esta sentencia no es coincidente con la finalmente consagrada en el RGPD: mientras que el derecho al olvido del artículo 17 RGPD es una aplicación del de derecho de supresión; el derecho consagrado con el mismo nombre por la jurisprudencia europea constituye una manifestación concreta del derecho de oposición. Veámoslo.

Esencialmente, el objeto del asunto, que responde a una cuestión prejudicial planteada por la Audiencia Nacional española, era delimitar si un ciudadano tiene, o no, derecho a exigir de los motores de búsqueda que dejen de incluir en la lista de resultados una información referida a su persona cuando la considere negativa o perjudicial para su persona, aun siendo lícita y exacta en su origen.

La respuesta del Tribunal europeo partió de la afirmación de que la actividad realizada por un motor de búsqueda, consistente en hallar información publicada o puesta en internet por terceros, indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», y, en consecuencia, el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento. Tal responsabilidad no resulta afectada por el hecho de que los editores o la fuente original de los contenidos «tengan la facultad de indicar a los gestores de los motores de búsqueda, con la ayuda, concretamente, de protocolos de exclusión como «robot.txt», o de códigos como «*noindex*» o «*noarchive*», que desean que una información determinada, publicada en su sitio, sea excluida total o parcialmente de los índices automáticos de los motores. En consecuencia, el motor de búsqueda está obligado a evitar la indexación de información referida a una persona, cuando esta considere que pueda perjudicarle, aunque la información no se borre previa o simultáneamente por la fuente original e incluso si la información publicada es en sí misma lícita. El TJUE llegó a esta conclusión realizando una interpretación amplia de los derechos de oposición al tratamiento y de cancelación de datos consagrados en la Directiva 95/46/CE.

En consecuencia, mientras que el derecho al olvido previsto en el art. 17 RGPD permitirá que el interesado exija a los editores de los contenidos que publican información personal la supresión de tales contenidos y la notificación a los motores de búsqueda del derecho de supresión ejercido para que dejen de indexarlos y de incluirlos

en la lista de resultados; el reconocido, con el mismo nombre en la Sentencia del TJUE de 13 de mayo de 2014, asunto C-131/12, es un derecho radicalmente distinto, que permite exigir directamente al motor de búsqueda la no inclusión en la lista de resultados de búsqueda por su nombre de determinados contenidos, ni la referencia ni el enlace a ellos por incluir información que puede perjudicar al interesad; esto es, manteniendo esos datos publicados, dado que no se impone al editor suprimirlos, simplemente se puede exigir dificultar su localización al prohibir su indexación.

Con posterioridad, la Sala de lo Contencioso-Administrativo de la Audiencia Nacional dictó sentencia, de fecha 29 de diciembre de 2014 (recurso número 725/2010) y la sentencia de la Sala de lo Civil, 4132/2015, de 15 de octubre de 2015, del Tribunal Supremo español (RJ 2015/4417) aplicaron la doctrina establecida en la cuestión prejudicial sobre el caso Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González. En esta última sentencia, el Tribunal Supremó delimitó los parámetros de ponderación de derechos y libertades informativas que corresponden a las denominadas hemerotecas digitales (art. 20.1 Constitución Española) y, de otro, los que corresponden a los sujetos titulares de los datos almacenados en ellos, acudiendo al criterio de «veracidad» de los datos. En concreto, el Tribunal Supremo rechaza la procedencia de eliminar los nombres y apellidos de la información recogida en la hemeroteca, o que los datos personales contenidos en la información no puedan ser indexados por el motor de búsqueda interno de la hemeroteca, pues considera que estas medidas supondrían una restricción excesiva de la libertad de información; en cambio, cuando los datos indexados afecten al honor («reputación») del titular de los datos, las hemerotecas digitales sí tendrán la obligación de impedir su localización del titular de los datos por «motores de búsqueda» externos.

En fase de redacción de este trabajo, con fecha de 4 de junio de 2018, el Tribunal Constitucional español, 58/2018 (recurso de amparo núm. 2096-2016), se ha pronunciado por primera vez sobre el derecho al olvido, matizando este aspecto, al estimar parcialmente un recurso de amparo contra la sentencia del Tribunal Supremo de 15 de octubre de 2015. El Tribunal Constitucional cuestiona el tratamiento diferencial en relación con el ejercicio del derecho al olvido entre un buscador interno de un periódico, aunque accesible por el público en general, y un motor de búsqueda de internet cuando la localización de la información se produce a partir de los datos personales del afectado. A este respecto advierte que la restricción del funcionamiento del motor de búsqueda interno –en caso de prohibir la indexación a partir de los nombres de los afectados- no excluiría el acceso a través del buscador a la información cuando se utilicen términos de búsqueda diferentes a los datos personales de los afectados. En este sentido, el Tribunal Constitucional pone de relieve que la prohibición de indexar los datos personales de los afectados también en el buscador interno del periódico debe considerarse una medida "idónea, necesaria y proporcionada", advirtiendo: "*debe tenerse en cuenta que los motores de búsqueda internos de los sitios web cumplen la función de permitir el hallazgo y la divulgación de la noticia, y que esa función queda garantizada aunque se suprima la posibilidad de efectuar la búsqueda acudiendo al nombre y apellidos de las personas en cuestión, que no tienen relevancia pública alguna. Siempre será posible, si existe una finalidad investigadora en la búsqueda de información alejada del mero interés periodístico en la persona*

«investigada», localizar la noticia mediante una búsqueda temática, temporal, geográfica o de cualquier otro tipo"[29].

3. CAMBIO DE PARADIGMA: LA CULTURA DE LA PRIVACIDAD COMO OBLIGACIÓN DE RESULTADO

El RGPD no ha modificado de manera sustancial los conceptos y principios básicos, pero sí el sistema de gestión de la privacidad por parte de responsables y encargados de tratamiento. De un modelo estático centrado en el dato personal y basado en el control del cumplimiento, con obligaciones tasadas (inscripción-notificación de creación, modificación o supresión de ficheros en el Registro de la correspondiente autoridad de control, documento de seguridad implementado, información, consentimiento, auditorías…), se pasa a otro que centra su atención en el uso que se realiza de los datos personales, para qué y cómo se utilizan, y que descansa en uno de los principios reseñados anteriormente, el principio de responsabilidad proactiva ("*accountability*"), conforme al cual, sin perjuicio de la existencia de aspectos reglados (obligatoriedad de realizar evaluaciones de impacto en ciertos supuestos de tratamientos, de designar un Delegado de Protección de Datos…), incumbe al responsable aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme a los principios de protección de datos, y además deberá garantizar disponer de los métodos de validación que garanticen la fiabilidad y efectividad de las medidas de seguridad implantadas al respecto. En este sentido, el RGPD fomenta la adhesión a códigos de conducta regulados en los artículos 40 y 41, o a un mecanismo de certificación contemplado en los artículos 42 y 43, que podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento (arts. 5 y 24 RGPD). En este misma línea, como se indicaba anteriormente, se pronuncian los EPDPEI (arts. 20 y 40).

La norma europea adopta un modelo menos rígido y menos tutelado, que exige a cualquier entidad u organización conocer el régimen jurídico de la protección de datos, realizar una reflexión o valoración previa sobre la afectación o riesgos a la privacidad que sus tratamientos puedan comportar, y adoptar las medidas que procedan para evitarlos. Partiendo de que en el nuevo sistema los operadores, responsables y encargados de tratamiento, disponen de una amplia libertad para organizar el tratamiento de los datos personales de la forma que estimen más adecuada para salvaguardar los derechos de los interesados, puede decirse que su responsabilidad pasa a ser por el resultado más que por los medios o diligencia que empleen[30].

---

[29] .- El texto de la sentencia puede consultarse en https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2018_060/2016-2096STC.pdf

[30] .- Consecuente con la gran libertad dejada a los responsables del tratamiento para organizar su política de protección de datos, el RGPD incorpora un régimen sancionador mucho más severo para el caso de que se incumplan sus prescripciones (RECIO GAYO, M., "Las sanciones en el RGPD: comentarios a las Directrices del Grupo de trabajo del artículo 29", *Diario La Ley*, n.º 12, Sección Ciberderecho, 29 de noviembre de 2017). El artículo 83 RGPD prevé que las empresas que infrinjan lo dispuesto por el

Ahora bien esto no debe hacer perder de vista que de la mano de este principio de responsabilidad proactiva derivan nuevas exigencias, algunas de las cuales han sido recogidas también de forma expresa en el capítulo VI de los EPDPEI bajo la rúbrica establecimiento de "*Medidas proactivas en el tratamiento de datos personales".* Serán examinadas a continuación, partiendo su regulación en el RGPD y resaltando los aspectos recogidos en los EPDPEI.

3.1. Privacidad desde el diseño y por defecto

Ambos conceptos[31] suponen para el responsable del tratamiento, tanto con carácter previo como durante el tratamiento, la necesidad de adoptar medidas de carácter técnico u organizativo que minimicen el número de datos personales tratados y aseguren que, por defecto, sólo se tratarán los datos personales imprescindibles y necesarios para cada objetivo o finalidad específica del tratamiento (art. 25 RGPD y 38 EPDPEI).

---

mismo, podrán ser sancionadas, dependiendo de la infracción que se cometa, con multas administrativas de hasta 20 millones de euros como máximo (o por un importe equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía). Como se advertido, a partir del 25 de mayo, el régimen sancionador establecido por el Reglamento General de protección de datos puede multiplicar por más de 1.000 el importe de las últimas sanciones impuestas a diferentes empresas (vid. FERNÁNDEZ, C. B., "De 300.000 euros a más de 2.000 millones de multa. Así se aplicará el nuevo régimen sancionador del RGPD", *Diario La Le*y, n.º 16, Sección Ciberderecho, 10 de abril de 2018, quien realiza una interesante comparativa calculando el importe que habrían alcanzado algunas de las más recientes y difundidas multas impuestas por la AEPD a conocidas empresas nacionales y extranjeras).

En este misma línea, como se indicaba anteriormente, se pronuncian los EPDPEI en su artículo 20, si bien remiten a la legislación nacional de los Estados iberoamericanos establecimiento de medidas correctivas y la sanción de las conductas, "indicando, al menos, el límite máximo y los criterios objetivos para fijar las correspondientes sanciones, a partir de la naturaleza, gravedad, duración de la infracción y sus consecuencias, así como las medidas implementadas por el responsable para garantizar el cumplimiento de sus obligaciones en la materia" (art. 43.3).

[31] .- Los términos «privacidad desde el diseño y por defecto» fueron acuñados a mediados de los años noventa del pasado siglo por Ann CAVOUKIAN, Comisionada de Información y Privacidad de la Autoridad de Protección de Datos de Ontario (Canadá), quien señala que la garantía de la privacidad debe convertirse por defecto en un modo de operar para cualquier organización. Este concepto se hace descansar en siete principios que deben ser aplicados a cualquier tratamiento de datos de carácter personal: 1. *Proactivo no Reactivo; Preventivo no Correctivo*: la privacidad desde el diseño se anticipa y previene eventos invasivos de privacidad antes de que sucedan; 2. *Privacidad como configuración predeterminada*: la privacidad desde el diseño busca entregar el máximo grado de privacidad asegurándose de que los datos personales estén protegidos automáticamente en cualquier sistema tecnológico dado o en cualquier práctica de negocios; 3. *Privacidad incrustada en el diseño;* 4. *Funcionalidad total – De suma positiva, no suma cero*: la privacidad desde el diseño busca acomodar todos los intereses y objetivos legítimos de una forma «ganar-ganar»; 5. *Seguridad extremo a extremo – Protección de ciclo de vida completo*: la privacidad desde el diseño garantiza una administración segura del ciclo de vida de la información, desde su inicio hasta su fin; 6. *Visibilidad y Transparencia*: la privacidad desde el diseño busca asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, están operando de acuerdo a las promesas y objetivos declarados, sujeta a verificación independiente; 7. *Respeto por la privacidad de los usuarios - Mantener un enfoque centrado en el usuario*: por encima de todo, la privacidad desde el diseño requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas (vid. CAVOUKIAN, A. *Privacy by Design The 7 Foundational Principles*. Revised: January 2011. Originally Published: August 2009, accessible en https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf).

La privacidad desde el diseño busca, como se indicado gráficamente, "encastrar" desde el origen la privacidad en sus productos, servicios, prácticas de negocio, sistemas de información, arquitecturas y redes de comunicación, implementando además mecanismos dirigidos a garantizar que, por defecto, su configuración recoge las opciones menos intrusivas y más protectoras de la privacidad para los usuarios[32].

3.2. Obligaciones de registro internas

Frente al marco normativo europeo hasta ahora vigente, que exigía la inscripción de ficheros de las organizaciones ante la Autoridad de control, la norma europea se centra en obligaciones de registro internas: cada responsable y encargado llevarán un Registro de las actividades de tratamiento efectuadas bajo su responsabilidad, que deberá contener una información de mínimos prevista en el artículo 30 RGPD y ser puesto a disposición de las autoridades de control en caso de ser solicitados.

No obstante, se trata de una obligación no aplicable "a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales" o datos personales relativos a condenas e infracciones penales.

Tales obligaciones de registro no aparecen recogidas en los EPDPEI.

3.3. Análisis y evaluaciones de riesgos

Como garantía de una gestión responsable de los tratamientos de datos de personas físicas, y con la finalidad de minimizar riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, derivados del tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales (problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo), el RGPD prevé la realización de dos tipos de análisis o evaluaciones de riesgos:

a) Análisis de riesgos. Corresponde a cualquier responsable y encargado del tratamiento llevar a cabo un análisis de riesgo de las operaciones de tratamiento de datos que realicen, con la finalidad de determinar si comportan un riesgo para los derechos y libertades de personas físicas (*ex art.* 32.1 RGPD) y adoptar medidas para mitigarlos (vgr., seudonimización consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro; cifrado de datos personales, para asegurar que un

[32].- Vid. OROZ VALENCIA, L., "Aproximación a la obligación de la protección de datos desde el diseño y por defecto*", Actualidad administrativa*, n.º 1, enero 2018, quien reseña, como ejemplo, la apertura de un perfil en una red social, donde el usuario por defecto ha de tener limitados todos los accesos de terceros y configuradas las máximas medidas de seguridad, y ha de ser el propio usuario quien, de forma voluntaria y consciente, haga la apertura de sus datos o elimine medidas de seguridad.

mensaje solo es entendible por el destinatario del mismo, mecanismos para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento…)

Evaluación de impacto relativa a la protección de datos o *privacy impact assessment* (PIA), *ex art.* 35 RGPD. Este segundo instrumento sólo resultará obligatorio si, tras la debida previa valoración, se ha llegado a la conclusión de que el tratamiento puede suponer un alto riesgo para los derechos y libertades de las personas físicas. Como supuestos *particulares*, el artículo 35.3 del RGPD describe tres casos que dan lugar a esos riesgos elevados:

> **a)** Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
>
> **b)** Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.
>
> **c)** Observación sistemática a gran escala de una zona de acceso público. En la primera propuesta que se publicó del RGPD se decía «c) el seguimiento de zonas de acceso público, en particular cuando se utilicen dispositivos optoelectrónicos (videovigilancia) a gran escala», por lo que podemos entender que «observación sistemática» es un concepto amplio que podría equivaler a «seguimiento» con cualquier tipo de dispositivo.

La evaluación de impacto deberá incluir como mínimo, conforme al art. 35.7:

a) «una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento (35.7.a) RGPD)
b) «una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad». Esto debe relacionarse con el considerando 39 del RGPD que indica que «los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios».
   Las autoridades de protección de datos a menudo señalan que para comprobar si una operación de tratamiento supone una medida restrictiva de un derecho fundamental, esta operación ha de superar los tres puntos del denominado juicio de proporcionalidad:
   — Si la medida puede conseguir el objetivo propuesto (juicio de idoneidad).
   — Si, además, es necesaria, en el sentido de que no hay otra más moderada para conseguir este propósito con la misma eficacia (juicio de necesidad).
   — Si la medida es ponderada o equilibrada para que se deriven más ventajas o desventajas para el interés general que no perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

c) «una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1», y
d) «las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas»

Los EPDPEI (art. 41) centran su atención exclusivamente en las evaluaciones de impacto como medida previa a la implementación por los responsables de tratamientos de datos que, por su naturaleza, alcance, contexto o finalidades, sea probable entrañen un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, remitiendo a la legislación nacional de los Estados Iberoamericanos aplicable la concreción, entre otros, de los siguientes aspectos:

- Tratamientos que requieran de una evaluación de impacto a la protección de datos personales;
- El contenido de la evaluación
- Los casos en que sea procedente presentar el resultado ante la autoridad de control, así como los requerimientos de dicha presentación

3.4. Delegado/Oficial de Protección de Datos

El RGPD prevé una figura de apoyo y asesoramiento al responsable o encargado a efectos de cumplimiento normativo, el Delegado de Protección de Datos (*Data Protection Officer, DPO*), atribuyéndole las siguientes funciones:

- Información y asesoramiento al responsable o al encargado del tratamiento de las obligaciones que les incumben;
- Supervisión del cumplimiento de lo dispuesto en el RGPD, las políticas del responsable o del encargado del tratamiento, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- Asesoramiento sobre la evaluación de impacto relativa a la protección de datos y supervisar su realización;
- Supervisión de las respuestas a las solicitudes de la autoridad de control y cooperar con la autoridad de control a solicitud de esta o por iniciativa propia;
- Actuación como punto de contacto de la autoridad de control para las cuestiones relacionadas con el tratamiento de datos personales.

Puede ser designado por cualquier responsable o encargado de tratamiento, pero será obligatorio en ciertos casos:

- El tratamiento de datos personales lo efectúe una autoridad u organismo público;
- Cuando las actividades principales del responsable o del encargado del tratamiento consistan en monitorizar al interesado, esto es, sean operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados a gran escala;
- Cuando "*las actividades del responsable o encargado consista en el tratamiento de categorías especiales de datos del artículo 9 (datos sobre el origen racial,*

convicciones religiosas, políticas, datos genéticos, de salud, condenas y delitos penales) a gran escala"[33].

El Delegado de Protección de Datos pueda ser un empleado del responsable o un profesional externo contratado, si bien su independencia, dentro de la Administración Pública o de la empresa, se refuerza al establecer expresamente la norma europea su capacidad para informar directamente a la dirección (sin recibir instrucción alguna), su incompatibilidad para cumplir otras funciones profesionales que puedan ocasionarle un conflicto de intereses y su inamovilidad durante un mandato mínimo de dos años, renovable sin límite, no pudiendo ser despedido ni sancionado por cumplir sus funciones[34].

Esta nueva figura de la normativa europea tiene su reflejo en el denominado por los Oficial de Protección de Datos personales establecido en el artículo 39 de los EPDPEI, que cuenta con similares funciones de asesoramiento, coordinación de las políticas de protección de datos del responsable y supervisión del cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia; y cuya designación, en paralelo como en la norma europea, se prevé obligatoria en los supuestos establecidos en las normativas nacionales o cuando:

- El responsable del tratamiento sea una autoridad pública;
- Se lleven a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular;
- Se realicen "*tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de*

[33] .- El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, actualmente en fase parlamentaria, multiplica hasta quince los casos en que será obligatoria su designación (artículos 34 a 37): (i) colegios profesionales y sus consejos generales, (ii) centros docentes y las Universidades públicas y privadas, (iii) entidades que exploten redes y presten servicios de comunicaciones electrónicas, cuando traten habitual y sistemáticamente datos personales a gran escala, (iv) prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio (v) entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito, (vi) establecimientos financieros de crédito, (vii) entidades aseguradoras y reaseguradoras sometidas a la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, (viii) empresas de servicios de inversión, reguladas por el Título V del texto refundido de la Ley del Mercado de Valores, (ix) distribuidores y comercializadores de energía eléctrica, conforme a lo dispuesto en la Ley 24/2013, de 26 de diciembre, del sector eléctrico, y los distribuidores y comercializadores de gas natural, conforme a la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos, (x) entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, (xi) entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos, (xii) centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, (xiii) entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas, (xiv) operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, y (xv) quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

[34] .- La AEPD ha publicado con fecha de 13 de junio de 2018 un Esquema de Certificación de Delegados de Protección de Datos, accesible en: https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf

los titulares, considerando, entre otros factores y de manera enunciativa más no limitativa, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen; el número de titulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de éstos".

4. FLEXIBILIDAD DE LOS FLUJOS TRANSFRONTERIZOS DE DATOS, PERO CON GARANTÍAS

El RGPD conserva, en lo esencial, el régimen de transferencias internacionales de datos dispuesto por la anterior Directiva 95/46/CE, es decir, la transmisión de datos personales a terceros países, territorios, sectores u organismos internacionales deberá estar respaldada por una decisión de la Comisión Europea que declare, conforme al artículo 45, que la legislación del Estado destinatario de los datos dispone de unos estándares de protección adecuados[35] ("nivel adecuado")[36] o, en otro caso, se aporten

[35] .- Bajo la vigencia de la Directiva 95/46/CE, la Comisión ha declarado como países con nivel adecuado de protección los siguientes: Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000; Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos; Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003; Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003; Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004; Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008; Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010; Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010; Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011; Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012; Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012. Tales Decisiones seguirán vigentes con el nuevo Reglamento hasta tanto no sean modificadas o derogadas.

Respecto de EEUU, tras la anulación por el Tribunal de Justicia de la Unión Europea, el pasado 6 de octubre de 2015, de la Decisión 2000/520 de la Comisión Europea que consideraba que los principios de *safe harbor* publicados por el Departamento de Comercio de EEUU el 21 de julio de 2000 garantizaban un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a empresas norteamericanas (Sentencia del Tribunal de Justicia -Gran Sala- de 6 de octubre de 2015. Asunto C-362/14), la Comisión Europea y los Estados Unidos acordaban, el 2 de febrero de 2016, un nuevo marco para los flujos transatlánticos de datos: Escudo de la privacidad Unión Europea – Estados Unidos: *Privacy Shield UE-EEUU.*

No obstante, en fase de conclusión de este trabajo, junio de 2018, el Comité de Libertades Civiles, Justicia e Interior del Parlamento Europeo (LIBE) ha hecho pública una resolución por la que propone que la Cámara solicite a la Comisión Europea que suspenda la aplicación del acuerdo *Privacy Shield* si EEUU no cumple con el mismo en su totalidad antes del próximo 1 de septiembre, y que dicha suspensión se mantenga hasta que las autoridades estadounidenses cumplan con los términos de dicho acuerdo en su totalidad (accesible en: http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf). En esta posición no ha sido ajeno el alcance y efectos lesivos evidenciados por el escándalo *Facebook-Cambridge Analytica*, compañías ambas certificadas bajo el *Privacy Shield*. Asimismo los eurodiputados han manifestado su preocupación por la reciente aprobación por parte de los Estados Unidos de la *Clarifying Lawful Overseas Use of Data Act* (Ley sobre Aclaración del Uso Legal de Datos en el Extranjero, conocida como *Cloud Act*), una norma que otorga a las autoridades de los EEUU acceso a datos personales alojados fuera de su país. Vid. nota de prensa en http://www.europarl.europa.eu/news/en/press-room/20180611IPR05527/eu-us-privacy-shield-data-exchange-deal-us-must-comply-by-1-september-say-meps

garantías suficientes (arts. 46 y 47), o se den algunas de las circunstancias previstas como excepciones (art. 49) en base a las cuales se considera legítimo transferir datos personales a terceros países de nivel no equiparable: consentimiento explícito del interesado; celebración o ejecución de un contrato o de medidas precontractuales entre interesado y el responsable; razones importantes de interés público[37]; formulación, el ejercicio o la defensa de reclamaciones; y protección de intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento[38].

En última instancia, esto es, cuando no exista ni decisión de adecuación, ni salvaguardas adoptadas ni sean de aplicación ninguna de las excepciones, solo se podrá llevar a cabo una transferencia internacional de datos a terceros países, si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evalué todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofrezca garantías apropiadas con respecto a la protección de datos personales. En este supuesto, se establece a cargo del responsable del tratamiento un deber de información, a parte de al interesado, a la autoridad de control de la transferencia[39].

---

[36] .- El documento del GT29 "*Adequacy Referential*", cuya versión final fue adoptada el 6 de febrero de 2018 (WP254rev.01), accesible en http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108, enumera aquellos principios que constituyen los pilares de la protección de datos y los requisitos «de procedimiento/de aplicación», cuyo cumplimiento pudiera considerarse mínimos para juzgar adecuada la protección. En cualquier caso, el RGPD establece que la Comisión deberá realizar revisiones periódicas, al menos cada cuatro años, que tengan en cuenta los desarrollos acaecidos en los países declarados adecuados. Si la revisión revelara que alguno de esos países no sigue asegurando un nivel adecuado de protección, la Comisión derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión (art. 45.3 RGPD)

[37] .- Además de intereses públicos como los recogidos en el artículo 23 RGPD (la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, interés económico o financiero, la sanidad pública y la seguridad social), el considerando 112 RGPD pone de relieve algunas manifestaciones del concepto de interés público, al señalar: "*Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. (…) Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados"*.

[38] .- Cuestión sobre la que se ha pronunciado el CEPD: Directrices 2/2018 del CEPD sobre las excepciones del artículo 49 del Reglamento 2016/679, adoptadas el 25 de mayo de 2018, accesibles en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

[39].- El artículo 48 RGPD hace una referencia al supuesto en que la transferencia esté motivada en una decisión por un órgano administrativo o judicial de un tercer país, procediendo si tiene su base en una de estas vías, bien en la existencia de un acuerdo internacional que reconozca o haga ejecutable tal decisión en la Unión Europea, como los *Mutual Legal Assistance Treaties*, bien cualquiera de los "*otros motivos para la transferencia"* previstos con carácter general en el RGPD.

A pesar de mantenerse en esencia el régimen de la Directiva 95/46/CE, se introducen una serie de cambios relevantes que flexibilizan el régimen de las transferencias, facilitando las relaciones económicas y la cooperación internacional fuera de la Unión Europea, pero al mismo tiempo garantizando los derechos de los afectados:

En primer lugar, se amplía el abanico de instrumentos que pueden incluir y aportar las garantías adecuadas para proteger los derechos de los afectados. Entre los que destacan:

a. Las cláusulas contractuales, bien aprobadas por la Comisión o por la autoridad de control –en cuyo caso la transferencia internacional no requiere autorización específica-, bien las establecidas *ad hoc* entre el responsable o el encargado y el destinatario de los datos, las cuales ofrecen una mayor flexibilidad aunque, a diferencia de las anteriores, deben ser autorizadas de manera específica previamente por la autoridad de control.

b. Se otorga reconocimiento legal a las Normas Corporativas Vinculantes (conocidas por sus siglas en inglés, BCRs, «*Binding Corporate Rules*») para los grupos multinacionales que, habían sido objeto de un amplio desarrollo por el GT29

c. Se incorporan los códigos de conducta y los mecanismos de certificación como instrumentos que pueden incorporar esas garantías. incertidumbre sobre los elementos que cada uno de estos dos mecanismos debe cumplir para ser considerados una garantía adecuada[40].

En segundo lugar, se reducen los supuestos que exigen autorización y notificación previa de las transferencias internacionales a una autoridad de control. Por lo general, en el nuevo marco europeo, las transferencias se pueden llevar a cabo sin necesidad de autorización previa, salvo que las garantías se aporten a través de un contrato *ad hoc* o de un acuerdo administrativo entre autoridades públicas; tampoco habrá necesidad de notificación a la autoridad de control, salvo que se amparen en la excepción basada en el interés legítimo imperioso del responsable del tratamiento. facilitar las relaciones comerciales y la cooperación internacional al evitar tener que solicitar la autorización de la Agencia en la mayoría de los casos, pero al mismo tiempo garantizando los derechos de los afectados en la transmisión de los datos fuera de la UE

Los EPDPEI dedican el capítulo V, integrado por el artículo 36, a las transferencias internacionales de datos. Los criterios adoptados siguen de cerca, con los oportunos matices, el modelo europeo.

Sin perjuicio de los límites a las transferencias internacionales que las legislaciones

[40] .- Precisamente uno de los primeros documentos emitidos por el Comité Europeo de Protección de Datos (CEPD), organismo de la Unión Europea previsto por el RGPD en sustitución del GT29, e integrado por los directores de las autoridades nacionales de control y el Supervisor Europeo de Protección de Datos, ha sido en este ámbito dadas las incertidumbres sobre los elementos que este mecanismo debe cumplir para ser considerado una garantía adecuada: Directrices 1/2018 del CEPD sobre certificación y criterios de certificación de acuerdo con los artículos 42 y 43 del Reglamento 2016/679, adoptadas el 25 de mayo de 2018, accesibles en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_1_2018_certification_en.pdf.

nacionales de los Estados iberoamericanos puedan establecer por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público, las transferencias internacionales de datos pueden encontrar su base legitimadora en:

----La adecuación, esto es, la existencia de un reconocimiento emitido, conforme a su legislación nacional, por el país transferente en cuanto a la adecuación del nivel de protección de datos del país destinatario, aunque también, a falta de este reconocimiento previo, pueden basarse en la acreditación por el destinatario de condiciones mínimas y suficientes para garantizar un nivel adecuado de protección de datos personales.

----A falta de adecuación, el exportador puede ofrecer garantías suficientes del tratamiento de los datos personales en el país destinatario, y éste, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado Iberoamericano. Como garantías se recogen:

. La suscripción cláusulas contractuales entre exportador y destinatario que permitan demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares, que pueden ser validadas por la autoridad de control conforme a lo establecido en la legislación nacional de los Estados Iberoamericanos.
. La adopción por exportador y destinatario de un esquema de autorregulación vinculante o un mecanismo de certificación aprobado, siempre y cuando éste sea acorde con las disposiciones previstas en la legislación nacional del Estado Iberoamericano, que está obligado a observar el exportador.

----A falta de los anteriores, la transferencia debe ser autorizada por la autoridad de control del Estado Iberoamericano del país del exportador, en los términos en su la legislación nacional

V. CONCLUSIÓN

El nuevo marco normativo de protección de datos europeo abre un amplio abanico de retos aplicativos a las organizaciones y entidades responsables o encargadas de tratamiento de datos personales que, sean o no europeas, pretendan operar en el mercado único. Su plena efectividad exige situar la cultura de protección de datos en el epicentro de cualquier organización, en el bien entendido sentido de que recopilar procesar y transferir datos de carácter personal no será ilegal, lo ilegal será hacer un uso inadecuado, generando situaciones insostenibles y desequilibradas para los derechos de las personas.

Ahora bien, en un entorno tecnológico global, no hay que obviar que los flujos internacionales de datos abogan por una búsqueda de soluciones globales en materia de privacidad, de ahí que el reto sea alcanzar unos estándares internacionales de protección de datos personales que desemboquen en un instrumento normativo universal y vinculante y, en este sentido, la norma europea pretende constituirse en el modelo de referencia.

Aunque el camino es largo, el consenso de unos principios comunes en la región iberoamericana, de la mano de la adopción de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, constituye un primer paso para la armonización de las legislaciones nacionales de la región en pro del ofrecimiento de mayores garantías a los ciudadanos en la protección de su derecho fundamental a la protección de datos y, sin duda, su armonización y convergencia con el marco normativo europeo constituirá un motor de desarrollo que favorezca las relaciones económicas entre ambos continentes.

BIBLIOGRAFÍA

AA.VV., *Protección de datos y habeas data: una visión desde Iberoamérica*, coord. por Daniel A. LÓPEZ CARBALLO. Agencia Española de Protección de Datos, 2015.

AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, dir. por José Luis PIÑAR MAÑAS, Ed. Reus, Madrid, 2017.

AA.VV., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, coord. por José LÓPEZ CALVO, Ed. Wolters Kluwer España, Madrid, 2018.

CAVOUKIAN, A. *Privacy by Design The 7 Foundational Principles.* Revised: January 2011.

FERNÁNDEZ, C. B., "De 300.000 euros a más de 2.000 millones de multa. Así se aplicará el nuevo régimen sancionador del RGPD", *Diario La Le*y, n.º 16, Sección Ciberderecho, 10 de abril de 2018

FOER, F., *Un mundo sin ideas. La amenaza de las grandes empresas tecnológicas a nuestra intimidad*, Ed. Paidós, Barcelona, 2017.

HAN, B., *La sociedad de la transparencia,* Ed. Herder, Barcelona, 2013.

HAN, B., *"En el enjambre"*, Ed. Herder, Barcelona, 2014.

LÓPEZ AGUILAR, J. F., "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del Derecho europeo, y su impacto en la relación transatlántica UE-EEUU", *UNED. Teoría y Realidad Constitucional*, núm. 39, 2017, pp. 557-581.

LÓPEZ CALVO, J., "Inteligencia Artificial y derecho de «explicación» en el Reglamento Europeo de Protección de Datos", *Diario La Ley*, n.º 16, Sección Ciberderecho, 10 abril 2018.

OROZ VALENCIA, L., "Aproximación a la obligación de la protección de datos desde el diseño y por defecto*", Actualidad administrativa*, n.º 1, enero 2018.

RECIO GAYO, M., “Las sanciones en el RGPD: comentarios a las Directrices del Grupo de trabajo del artículo 29”, *Diario La Ley*, n.º 12, Sección Ciberderecho, 29 de noviembre de 2017.