CONSTITUCIONAL-ADMINISTRATIVO

Algunas novedades en la protección de datos a la luz del nuevo marco normativo

Juan Panisello Martínez
Abogado

Este trabajo ha sido seleccionado para su publicación por: don Francisco Monterde Ferrer, don Fernando Calancha Marzana, doña Silvia Díez Sastre, don Julio V. González García, don Luis Medina Alcoz y don José Vicente Morote Sarrión.

Extracto

Estamos viviendo una auténtica revolución tecnológica, con un incremento diario exponencial de datos. El flujo de información es continuo, masivo y además global. Las nuevas posibilidades de acumulación de datos y de elaboración de perfiles comportan una mayor capacidad de control sobre los individuos. La normativa debe tener por objeto proteger a las personas frente a las empresas que almacenan y negocian con los datos de las personas, por lo que compete al legislador lograr un óptimo equilibrio entre la salvaguardia de la vida privada y el interés progresivo que tiene la sociedad en el tráfico de la información sobre las personas, información que se ha convertido en una mercancía muy valiosa. En materia de protección de datos la aprobación del nuevo Reglamento Europeo de Protección de Datos supone una nueva cultura de la privacidad en un mundo de redes sociales, teléfonos inteligentes, banca por internet y transferencias globales.

Palabras clave: protección de datos; privacidad; seguridad; certificación.

Fecha de entrada: 03-05-2017 / Fecha de aceptación: 04-07-2017 / Fecha de revisión: 29-04-2018

Some new developments in the protection of data in the light of the new normative framework

Juan Panisello Martínez

Abstract

We are experiencing a real technological revolution, with an exponential daily increase in data. The flow of information is continuous, massive and also global. The new possibilities of data accumulation and profiling imply a greater capacity for control over individuals. The regulation should aim to protect people against the companies that store and negotiate with the data of the people, so it is the responsibility of the legislator to achieve an optimal balance between safeguarding privacy and the progressive interest that society has in the traffic of information about people, information that has become a very valuable commodity. In terms of data protection, the adoption of the new European Data Protection Regulation is a new culture of privacy in a world of social networks, smart phones, internet banking and global transfers.

Keywords: data protection; privacy; security; certification.

Sumario

Cómo citar este estudio:

Panisello Martínez, J. (2018). Algunas novedades en la protección de datos a la luz del nuevo marco normativo. *Revista Ceflegal, 209*, 63-96.

I. CUESTIONES PREVIAS

Cuando en el año 1978 el artículo 18 de la Constitución Española (CE) garantizaba los derechos fundamentales al honor y a la intimidad, si bien hacia una clara referencia a la limitación, mediante ley, del uso de la informática[1], posiblemente nadie era consciente de la repercusión que en el futuro iban a tener las nuevas tecnologías de la información[2] y la comunicación[3]. Sin perjuicio de que los citados derechos fundamentales mantienen su autonomía en virtud de su explicita mención en el artículo 18 de la CE, convendría apreciarlos como instrumentos de tutela y protección de distintas facetas de un mismo bien jurídico: la vida privada de las personas, cuya protección no debe limitarse a la protección de la intimidad[4], pues de lo contrario en ocasiones resulta difícil establecer cuál es el derecho fundamental que resulta vulnerado[5].

El creciente desarrollo tecnológico de los sistemas de comunicación, información, técnicas de captación y grabación de sonido e imagen comporta nuevos e interesantes problemas jurídicos[6], obligándonos a elaborar normas, nacionales e internacionales, para garantizar la vida privada de las personas[7], así como para proteger su derecho a la autodeterminación informativa[8].

---

1 Morais Gallego, J. P. (marzo 2006). Las nuevas tecnologías de la información y de la comunicación. Implicaciones legales. *Revista Galega do Ensino*, *48*, 431 (consultado el 5 de septiembre de 2016).

2 De Carreras Serra, Ll. (1996). *Régimen jurídico de la información. Periodistas y medios de comunicación* (p. 62). Barcelona: Ariel Derecho,

3 Morais Gallego, J. P. (marzo 2006, p. 431).

4 De Carreras Serra, Ll. (1996, pp. 71 y 82).

5 STC 110/1984, de 26 de noviembre (FJ 3) (NFJ000067).

6 Ordóñez Solís, D. (2011). *Privacidad y protección judicial de los datos personales* (p. 14). Bosh.

7 STC 254/1993, de 20 de julio (NFJ068942), indica (FJ 7) que «la protección de la intimidad de los ciudadanos requiere que estos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades».

8 Lucas Murillo de la Cueva, P. (abril-junio 1999). La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos (Nueva Época)*, *104*, 35 y ss.

El llamado derecho a la autodeterminación informativa se fraguó con la sentencia sobre la Ley del Censo[9], dictada por el Tribunal Constitucional Federal alemán, en la que se afirmaba que el derecho general de la personalidad comporta la atribución al individuo de la capacidad de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar de su propia vida[10]. La consecuencia de este razonamiento es el reconocimiento jurisprudencial de un derecho fundamental a la autodeterminación informativa[11] basado en el derecho general de la personalidad, ofreciendo protección frente a la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos de carácter personal, y garantizando la facultad del individuo de decidir básicamente por sí mismo sobre la difusión y la utilización de sus datos personales[12].

En España el derecho fundamental a la protección de datos, inicialmente denominado «libertad informática»[13], se estableció de manera confusa[14], si bien, con posterioridad, la jurisprudencia[15] fue perfilando su contorno[16] al reconocer una capacidad de control a las personas sobre los datos de carácter personal que les conciernen[17]. No obstante, a pesar de que en la actualidad el derecho a la protección de datos se encuentra plenamente reconocido e integrado en el orde-

9 Traducida por Manuel Daranas (enero, 1984). *Boletín de Jurisprudencia Constitucional* (p. 33).

10 Heredero Higueras, M. (1983). La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983. *Documentación Administrativa*, *198*, 139 a 158.

11 Lucas Murillo de la Cueva, P. (abril-junio 1999, pp. 35 y ss).

12 Pérez Luño, A. E. (1996). *Manual de informática y derecho* (p. 43). Barcelona: Ariel; Pérez Luño, A. E. (1989). Libertad informática y derecho a la autodeterminación informativa. *I Congreso sobre Derecho Informático* (p. 359 a 375). Universidad de Zaragoza.

13 STC 254/1993 (FJ 6) (NFJ068942) y otras SSTC 143/1994 (FJ 7) (NFJ003358), 11/1998 (FJ 4) (NSJ002117), 94/1998 (FJ 6) (NSJ003080), o 202/1999 (FJ 2).

14 Villaverde Menéndez, I. (mayo-agosto 1994). Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993 (NFJ068942). *Revista Española de Derecho Constitucional*, *41*, 187 a 224.

15 STC 143/1994 (NFJ003358), de 9 de mayo, relativa a las normas reguladoras del número de identificación fiscal; la STC 11/1998 (NSJ002117), de 13 de enero, declaró contrario a la libertad sindical, en relación con el artículo 18.4 de la CE, el uso por una empresa del dato de la afiliación sindical para detraer haberes de los trabajadores con ocasión de una huelga promovida por determinado sindicato [doctrina reiterada resolviendo idéntica cuestión en STC 94/1998 (NSJ003080), de 4 de mayo, entre otras]; la STC 202/1999, de 8 de noviembre, con ocasión de la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de una entidad de crédito sobre bajas por incapacidad temporal, apreció que el almacenamiento sin cobertura legal en soporte informático de los diagnósticos médicos del trabajador sin mediar su consentimiento expreso constituía una desproporcionada restricción del derecho fundamental a la protección de datos personales; y en especial STC 292/2000, de 30 de noviembre (FJ 5) (NCJ051718), que trae causa del recurso de inconstitucionalidad que interpuso el Defensor del Pueblo, contra incisos de los artículos 21.1 (Comunicación de datos entre Administraciones públicas) y 24.1 y 2 (Otras excepciones a los derechos de los afectados) de la LOPD, por vulneración de los artículos 18.1 y 4 y 53.1 de la CE.

16 Lucas Murillo de la Cueva, P. (2003). La primera jurisprudencia sobre el derecho a la autodeterminación informativa», *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, *1*.

17 Piñar Mañas, J. L. (2009). Protección de Datos: origen, situación actual y retos de futuro. En P. Lucas Murillo de la Cueva y J. L. Piñar Mañas, *El Derecho a la Autodeterminación Informativa* (p. 93). Madrid: Fundación Coloquio Jurídico Europeo.

namiento jurídico[18] y plenamente consolidado como derecho fundamental autónomo[19], cada día son mayores los riesgos de su vulneración en la sociedad actual[20].

II. NUEVO MARCO NORMATIVO

Después de casi 40 años de la entrada en vigor de la CE de 1978, y sabida ya la derogación el 25 de mayo de 2018[21] de la Directiva 95/46/CE[22], que junto con el Convenio 108 del Consejo de Europa[23] y las directrices de la OCDE de 1980[24] revolucionaron la protección de datos a nivel mundial[25], debemos prestar atención al nuevo paradigma en la protección de datos personales que se vislumbra con el nuevo 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 (Reglamento de Protección de Datos, en adelante RPD), que entró en vigor el 25 de mayo de 2016 y será de obligatorio cumplimiento el 25 de mayo de 2018[26].

Tras el acuerdo alcanzado por el Consejo, el Parlamento y la Comisión el 15 de diciembre de 2015, el Comité de Representantes Permanentes (COREPER) el 18 de diciembre de 2015 confirmó los textos transaccionales acordados con el Parlamento Europeo (PE) sobre la reforma de la protección de datos. Con posterioridad, tras más de cuatro años de trabajo para reformar drásticamente la normativa comunitaria sobre protección de datos, el PE el 14 de abril de 2016 aprueba el texto consensuado del nuevo RPD, el cual supone una nueva cultura de la privacidad en un mundo de las redes sociales, los teléfonos inteligentes, la banca por internet y las transferencias globales[27].

---

18 De Carreras Serra, Ll. (1996, p. 62.)

19 Villaverde Menéndez, I. (mayo-agosto 1994, pp. 187 y ss.); González Murúa, A. R. (1994). Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales. *Revista Vasca de Administración Pública*, *37*, 227 y ss.; y Arroyo Yanes, L. M. (1993). El Derecho de Autodeterminación Informativa frente a las Administraciones Públicas (Comentario a la STC 254/93, NFJ068942, de 20 de julio). *Revista Andaluza de Administración Pública*, *16*, 119 y ss.

20 Aberasturi Gorriño, U. (2013). El derecho a la indemnización en el artículo 19 de la ley orgánica de protección de datos de carácter personal. *Revista Aragonesa de Administración Pública*, *41-42*, 174.

21 Artículo 99 del RPD.

22 Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

23 Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981 adoptado en Estrasburgo.

24 Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (1980).

25 Piñar Mañas, J. L. (junio 2016). Reglamento europeo de protección de datos: retos y oportunidades para la abogacía. *Revista del Consejo General de la Abogacía*, *98*, 27.

26 Publicado en el Diario Oficial de la Unión Europea el 4 de mayo de 2016 (consultado el 5 de julio de 2016).

27 En este sentido puede consultarse la web del Consejo de la Unión Europea, Reforma de la protección de datos (consultado el 4 de octubre de 2016).

En todo caso, su objetivo no es otro que mejorar el nivel de protección de los datos de las personas físicas cuyos datos personales se someten a operaciones y procesamiento automatizado o no; así como aumentar las oportunidades de negocio y libertad de movimiento en el mercado único digital, particularmente mediante la reducción de la burocracia administrativa[28].

Como datos relevantes a tener en consideración mencionar que al 70 % de los europeos les preocupa que las empresas puedan utilizar la información para fines diferentes de aquellos para los que se recogió, que el 57 % consideran que la divulgación de información personal es una cuestión importante, que solo el 15 % supone que controla completamente la información que aporta en línea y que el 90 % de los europeos cree que es importante que en todos los países de la Unión Europea (UE) se tengan los mismos derechos y la misma protección[29].

En cuanto a la convivencia del derecho de la UE y el derecho nacional, convendremos que la Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (LOPD) podrá seguir siendo aplicable en lo que esté fuera del Derecho de la UE, por lo que si bien no podrá considerarse derogada, sí podrá considerarse desplazada por la normativa europea[30]. Si bien en apoyo de lo afirmado tal vez sea suficiente señalar que el propio RPD hace numerosas remisiones a la legislación nacional de los Estados miembros[31], no es menos cierto que se nos pueden plantear dudas en algunas cuestiones: ¿habrá que seguir realizando el registro de ficheros en nuestro país por efecto de la LOPD o cabe entender una derogación tácita de sus disposiciones en este sentido?, o ¿qué valor tendrán la circulares de la Agencia Española de Protección de Datos (AEPD) en el nuevo contexto[32]?

III. ALGUNAS NOVEDADES

El nuevo RPD presenta importantes novedades[33] en la regulación de la protección de datos de carácter personal[34], algunas de la cuales, *grosso modo*, pasamos a indicar[35]: la definitiva con-

28 Véase el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea, y el artículo 16.1 del TFUE, pues toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

29 En este sentido, European Commission (2015). Data protection. *Special Eurobarometer 431*, European Union, (consultado el 5 de septiembre de 2016).

30 Piñar Mañas, J. L. (junio 2016, p. 26).

31 A título de ejemplo, artículo 83.7 del RPD, relativo a las multas administrativas que pueden imponer los Estados.

32 Carlos FH-Redacción Noticias Jurídicas (4 de mayo de 2016). Contenido y novedades del Reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016) (consultado el 20 de octubre de 2016).

33 Piñar Mañas, J. L. (junio 2016, p. 26).

34 En este sentido, Lavanguardia.com (30 de septiembre de 2016): Una nueva cultura de la privacidad. El nuevo reglamento de protección de datos presenta novedades que dan respuesta al tratamiento de la información personal que se hace en la red (consultado el 17 de octubre de 2016).

35 Piñar Mañas, J. L. (junio 2016, p. 27).

solidación de la protección de datos como derecho fundamental; la extensión del ámbito territorial de aplicación de las normas protectoras de la privacidad[36]; la definición y regulación del consentimiento del interesado[37]; el principio de transparencia[38] que inspira la norma se materializa, entre otros, en el principio de información al interesado que pasa a ser tratado como un derecho a la información[39]; la regulación del derecho al olvido[40] y del derecho a la portabilidad de datos[41], así como del derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados de datos, en el que se hace una referencia expresa a la elaboración de perfiles[42]; la incorporación decidida del principio de responsabilidad[43]; la exigencia de tener en cuenta los principios de privacidad desde el diseño y por defecto[44]; la no necesidad de inscribir los ficheros, aunque sí sea necesario que los responsables y encargados lleven un registro de las actividades del tratamiento, que estará a disposición de las autoridades de control[45]; la importantísima obligación de notificar las violaciones de seguridad[46]; la regulación de la evaluación de impacto relativa a la protección de datos[47] y la consulta previa al tratamiento si este entraña un alto riesgo[48]; el impulso a la autorregulación mediante la creación de códigos de conducta[49], y al establecimiento de mecanismos de certificación y sellos y marcas de protección de datos[50]; la más precisa regulación de las transferencias internacionales con una referencia expresa a las normas corporativas vinculantes como legitimadoras de las transferencias[51]; el régimen de las autoridades independientes de control[52] y el enrevesado mecanismo de cooperación y coherencia[53]; la nueva

36 Artículo 3 del RPD.

37 Artículos 4.11 y 7 del RPD, respectivamente.

38 Artículo 12 del RPD.

39 Artículos 13 y 14 del RPD.

40 Artículo 17 del RPD.

41 Artículo 20 del RPD.

42 Artículo 22 del RPD.

43 Artículo 24 del RPD.

44 Artículo 25 del RPD.

45 Artículo 30 del RPD.

46 Artículo 33 del RPD.

47 Artículo 35 del RPD.

48 Artículo 36 del RPD.

49 Artículos 40 y 41 y Cdos. 98 y 99 del RPD.

50 Artículos 42 y 43 y Cdo. 100 del RPD.

51 Artículo 47 del RPD.

52 Artículos 51 a 59 del RPD.

53 Artículos 60 a 67 del RPD.

regulación del Comité Europeo de Protección de Datos[54], así como el derecho a la reclamación y recurso ante la autoridad de control o ante el responsable o el encargado del tratamiento[55]; y el derecho a la indemnización y responsabilidad[56].

Dicho lo anterior, a continuación nos fijaremos en algunas de las diversas novedades acabadas de apuntar.

1. ÁMBITO DE APLICACIÓN TERRITORIAL

Delimitar el ámbito de aplicación internacional de la legislación europea en materia de protección de datos resulta de gran importancia para los proveedores de buscadores y de servicios de redes sociales cuyo principal establecimiento se encuentre fuera de la UE[57], así como para la tutela de las personas afectadas por sus actividades[58].

En cuanto a lo novedoso en relación con el ámbito territorial de aplicación del RPD apreciamos una importante extensión del mismo, ya que[59]:

a) El RPD se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la UE, con independencia de que el tratamiento tenga lugar en la UE o no.

b) El RPD se aplica al tratamiento de datos personales de interesados que residan en la UE por parte de un responsable o encargado no establecido en la UE, cuando las actividades de tratamiento estén relacionadas con alguno de los siguientes aspectos:

b.1) La oferta de bienes o servicios a dichos interesados en la UE, independientemente de si a estos se les requiere su pago[60]. Es decir, con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del RPD, el tratamiento de datos personales de in-

54 Artículos 68 a 76 del RPD.

55 Artículos 77 a 79 del RPD.

56 Artículo 82 del RPD.

57 De Miguel Asensio, P. A. (2012). Buscadores de Internet y protección de datos: La cuestión prejudicial de la Audiencia Nacional sobre Google. *La Ley*, *7870*, 1 a 3. Disponible en <http://eprints.ucm.es>.

58 De Miguel Asensio, P. A. (2015). Aspectos internacionales de la protección de datos: Las sentencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley Unión Europea*, 1 a 10. Disponible en <http://eprints.ucm.es>.

59 Cdos. 36, 80 y artículo 3 del RPD.

60 Cdo. 23 del RPD.

teresados que residen en la UE por un responsable o un encargado no establecido en la UE debe regirse por el RPD si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Indicar que hay factores que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la UE, como son, por ejemplo:

- El uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o
- La mención de clientes o usuarios que residen en la Unión.

b.2) El control de su comportamiento, en la medida en que este tenga lugar en la UE[61]. Es decir, para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

c) El RPD se aplica al tratamiento de datos por parte de un responsable que no esté establecido en la UE, sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público, lo que amplía de forma considerable su ámbito de aplicación[62].

En definitiva, advertimos que se está posibilitando que el RPD sea aplicable a empresas que, hasta este momento, podían estar tratando datos de personas en la UE y que, sin embargo, se regían por normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea. En este sentido, y a modo de ejemplo, indicar que ahora será posible aplicar la normativa a cualquier oferta de bienes o servicios que se haga y que tenga por destino residentes de la UE. ¿Y eso en qué se traduce? En que a una oferta de bienes y servicios, con independencia de que esté hecha desde los Estados Unidos o Asia, se le podrá aplicar la normativa europea si se puede concluir que iba dirigida a ciudadanos europeos[63]. Este hecho permitirá hacer frente a la filtración en materia de protección de datos que se cometía fuera del territorio de la UE[64].

61 Cdo. 24 del RPD.

62 Cdo. 25 del RPD.

63 Piñar Mañas, J. L. (junio 2016, p. 27).

64 Cdos. 23 y 80 del RPD.

2. CONSENTIMIENTO DEL INTERESADO

Los principios y normas sobre el tratamiento de los datos personales[65] de las personas físicas se fundamentan en el respeto de los derechos y libertades fundamentales, en particular del derecho a la protección de los datos de carácter personal, el cual ha sido reforzado con la finalidad de proteger a las personas físicas cuyos datos se someten a procesamiento y asegurar en la práctica un mayor control sobre sus datos personales[66].

Los principios relativos al tratamiento de datos personales que formula y actualiza el RPD a destacar son: la licitud del tratamiento[67], el consentimiento necesario para el tratamiento de datos[68], las condiciones aplicables al consentimiento del menor[69], las categorías especiales de datos personales[70] y el tratamiento de datos relativos a condenas e infracciones penales[71].

Mención especial entendemos merece el consentimiento del interesado[72] para el tratamiento de datos, pues a diferencia de la actual LOPD, en la que el consentimiento puede ser tácito siempre que no se trate de datos sensibles, el RPD establece que el consentimiento habrá de ser expreso[73], sean cuales sean los datos tratados[74], y deberá ser[75]:

- Una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen. Puede ser una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.
- Para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para

65 Artículo 5 del RPD.

66 Cdo. 18 del RPD, indica que el «Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial».

67 Artículo 6 del RPD.

68 Cdo. 11 y artículo 7 del RPD.

69 Artículo 8 del RPD.

70 Artículo 9 del RPD.

71 Artículo 10 del RPD.

72 Artículo 4.11 del RPD.

73 Como indica el Cdo. 32 del RPD, el consentimiento debe darse mediante un acto afirmativo claro.

74 Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016). Hacia la seguridad de los datos después del Reglamento Europeo. *Jornadas Técnicas de RedIRIS 2016*, pp. 6 y 7 (consultado el 21 de enero de 2017).

75 Cdos 32 y 42 y artículo 7 del RPD.

> todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta[76].

Cuando el tratamiento de datos personales se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En este sentido podemos destacar, a modo de ejemplo, como consentimiento afirmativo: una casilla de un sitio web en internet, escoger ciertos parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra conducta o aclaración que indique claramente que el interesado acepta la propuesta del tratamiento de sus datos de carácter personal[77].

Además, la nueva normativa garantiza que cualquier ciudadano pueda dirigirse a la autoridad de control competente de su país para denunciar cualquier infracción que se haya cometido respecto a sus datos personales. Supongamos, a modo de ejemplo, que una empresa irlandesa que ofrece servicios a ciudadanos españoles infringe la normativa europea. El RPD garantizaría la intervención de la autoridad irlandesa, que sería la líder porque es allí donde está asentada la entidad, pero el ciudadano podría presentar una denuncia ante la AEPD. Y, además, quien le notificaría la resolución adoptada también sería, en este caso, la AEPD. Y esto es relevante, porque el hecho de que la resolución se tome en España posibilita al ciudadano impugnar con posterioridad la decisión ante los tribunales españoles[78].

3. OLVIDO DIGITAL

El RPD regula de manera expresa el derecho de supresión[79] o «derecho al olvido»[80], que se configura por vez primera como un derecho autónomo a los denominados «derechos ARCO»[81],

---

76 Palma Villalón, M. del V. (1 de mayo de 2016). Lo esencial del nuevo Reglamento Europeo de protección de datos aprobado por el Parlamento Europeo. *Revista Transformación Digital* (consultado el 22 de diciembre de 2016).

77 González Tapia, M. L. (14 de julio de 2016). Las casillas de marcación: El consentimiento para fines adicionales en la normativa de protección de datos. *Noticiasjuridicas.com* (consultado el 17 de octubre de 2016).

78 En este sentido, Lavanguardia.com (30 de septiembre de 2016).

79 Cdos. 65, 66 y 156 y artículos 17 y ss. del RPD.

80 Díaz Díaz, E. (2014). Los ciudadanos ante el «derecho al olvido». *Actualidad Jurídica Aranzadi*, *886*, parte Comentario, Aranzadi. Westlaw BIB 2014\1763; y Palma Villalón, M. del V. (1 de mayo de 2016).

81 Álvarez Hernando, J. y Cazurro Barahona, V. *Ejercicio de derechos de acceso, rectificación, cancelación y oposición (arco). Derecho al olvido en internet*. Grandes Tratados, Aranzadi. Westlaw BIB 2014\8354.

el cual ya había sido objeto de reconocimiento[82] por la jurisprudencia europea[83] y nacional[84], que tiene por objeto garantizar el derecho de los sujetos titulares de los datos a obtener, sin dilación indebida, la supresión de los datos personales que le conciernan del responsable del tratamiento en determinados supuestos[85], entre otros, cuando el demandante no es una persona de relevancia pública, ni los hechos presentan un interés histórico[86], cuando los datos personales hayan sido tratados ilícitamente[87]o cuando los datos personales deban suprimirse para cumplir con una obligación legal establecida en la legislación aplicable al responsable del tratamiento o cuando los datos no sean necesarios para las finalidades para las que fueron recogidos[88].

Además, este derecho supone que el interesado podrá reclamar que se bloqueen en las listas de resultados de los buscadores los vínculos que conduzcan a informaciones que le afecten que resulten, entre otros motivos, obsoletas, incompletas, falsas o irrelevantes y no sean de interés público[89].

No obstante, también resulta relevante destacar que este derecho incide en la esfera del responsable del tratamiento[90], pues deberá optar entre limitar el tratamiento[91], o bien suprimir sin demora la información[92], ponderando caso por caso el alcance de este derecho con el derecho a

---

82 Rallo Lombarte, A. (2014). La garantía del «derecho al olvido» en internet. *Actualidad Jurídica Aranzadi*, *886*, parte Comentario. Westlaw BIB 2014\1761.

83 STJUE, Gran Sala, de 13 de mayo de 2014, asunto C-131/2012, procedimiento entre Google Spain, S.L., Google Inc. y AEPD, disponible en <http://curia.europa.eu>.

84 STS 545/2015, de 15 de octubre de 2015 (ROJ: STS 4132/2015).

85 Moya Izquierdo, S. y Crespo Vitorique, I. (2014). Los motores de búsqueda y el «derecho al olvido» cuando la tecnología avanza más rápido que el Derecho. *Unión Europea Aranzadi*, *10*, 27 a 37. Aranzadi y Rallo Lombarte, A. (2011). La privacidad en la era digital: El derecho al olvido. *Actualidad Jurídica Aranzadi*, *815*, parte Tribuna, Aranzadi. Westlaw BIB 2011\273.

86 Martínez Bavière, J. y Menéndez-Abascal Cabiedes, S. (24 de noviembre de 2015). El Tribunal Supremo precisa el alcance del «derecho al olvido» frente a los medios de comunicación. *Elderecho.com* (consultado el 4 de julio de 2016).

87 Roldán Aguirre, I. (2016). Criterios del «derecho al olvido» en los buscadores de internet. *Revista Aranzadi Doctrinal*, 6, parte Fichas de Jurisprudencia. Aranzadi. Westlaw BIB 2016\3059.

88 Para un estudio con más profundidad del «derecho al olvido digital» puede consultarse: Simón Castellano, P. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayo de 2014*. Bosch; y Álvarez Caro, M. (2015). *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*. Editorial Reus.

89 Rubio Torrano, E. (2016). El derecho al olvido digital. *Revista Doctrinal Aranzadi Civil-Mercantil*, *1*, parte Comentario, Aranzadi. Westlaw BIB 2015\18280.

90 Esto es, la entidad, corporación, sitio web o red social que trata los datos.

91 Artículo 18 del RPD.

92 Artículo 17 del RPD.

la libertad de expresión, la salud pública, el deber de conservación de los datos para dar cumplimiento a una obligación legal y el interés público[93].

4. PORTABILIDAD DE DATOS

Con el derecho a la portabilidad de datos[94] cualquier ciudadano europeo puede exigir a las empresas que estén tratando sus datos que se los devuelvan o que los transfieran a otra empresa[95], en un formato estructurado, inteligible[96] y automatizado[97], incluyendo tanto los datos proporcionados de manera consciente y activa por su titular, como los datos personales generados por su propia actividad, por lo que este derecho no queda limitado a la información personal comunicada de manera directa[98]. Así lo establece la nueva directriz europea aprobada por el Grupo de Trabajo del Artículo 29 (GT 29)[99], el cual también estableció como una buena práctica que los responsables del tratamiento de datos comenzasen a desarrollar los medios técnicos necesarios para atender las solicitudes de portabilidad de datos, a través de las necesarias herramientas de descarga y las interfaces de usuario apropiadas[100]. En todo caso advertir que, en la práctica, el ejercicio de este derecho habrá de ponderarse con los casos de tratamiento de datos personales que resulten necesarios para el cumplimiento de misiones de interés público, como puede ser, a modo de ejemplo, en el caso de la Administración tributaria o de justicia, o los inherentes al ejercicio del poder público conferidos al responsable del tratamiento, como, por ejemplo, en el caso del ejercicio de competencias expropiatorias o sancionadoras[101].

---

93 Sobre la aplicación práctica y los criterios de ponderación, *Guide lines on the implementation of the Court of Justice of the European Union judgmenton «Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12*, (NCJ058436) article 29 data protection working party, WP225, Adopted on 26 November 2014 (consultado el 6 de septiembre de 2016).

94 Artículo 20 del RPD, relativo al derecho a la portabilidad de los datos.

95 STC 292/2000 (NCJ051718), de 30 de noviembre, ya nos hacía entrever el derecho a la portabilidad (al igual que, en su caso, el derecho al olvido) cuando nos indicaba, en referencia a los derechos ARCO, que «el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales», atribuyendo «a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos».

96 Es decir, de uso común.

97 Es decir, legible por máquina.

98 Sobre el derecho a la portabilidad, *Guidelines on the right to data portability*, article 29 data protection working party, Adopted on 13 December 2016 (consultado el 20 de enero de 2017).

99 Organismo consultivo que reúne, entre otras instituciones, a las autoridades de Protección de Datos de todos los estados de la Unión Europea.

100 En este sentido El Derecho.com (5 de enero de 2017). El Derecho a la Portabilidad no está limitado a los datos comunicados de manera directa por su titular (consultado el 18 de enero de 2017).

101 Sobre el derecho a la portabilidad, *Guidelines on the right to data portability*, article 29 data protection working party, Adopted on 13 December 2016 (consultado el 20 de enero de 2017).

El derecho a la portabilidad de datos es también una herramienta importante que fomentará el libre flujo de datos personales en la UE, avivará la competencia entre controladores y promoverá el desarrollo de nuevos servicios en el contexto de la estrategia del mercado único digital. No obstante, no todo son ventajas ya que también puede plantear ciertos problemas de seguridad, como pueden ser, a modo de ejemplo, cómo garantizar la entrega de los mismos de forma segura a la persona adecuada o cómo asegurar su almacenamiento en los sistemas determinados[102].

5. RESPONSABILIDAD Y PRIVACIDAD

Con la nueva normativa el RPD introduce un cambio de paradigma en la forma de garantizar la protección de los datos. A modo de ejemplo, podemos fijarnos en las medidas de seguridad y la obligación de inscripción de ficheros[103]:

- En cuanto a la inscripción de ficheros. La actual LOPD española dispone la necesidad de notificar a la AEPD todos aquellos ficheros con datos de carácter personal que existan en nuestra organización[104]. Por contra, el nuevo RPD europeo nos exime de dicha obligación, pero, eso sí, nos obliga a llevar internamente un «registro de actividades de tratamiento» que deberemos poner a disposición de la autoridad de control por si nos fuere requerido.
- En cuanto a las medidas de seguridad. La actual normativa española regula tres niveles diferenciados: el básico, medio y el alto, en función del tipo de datos tratados y con medidas muy concretas para cada uno de estos niveles[105]. En cambio el nuevo RPD europeo nos dispensa de tal clasificación y medidas concretas, dejando, una vez más, en nuestras manos la fijación de las medidas concretas de seguridad que aplicamos sobre los datos pero debiendo, eso sí, justificar su pertinencia y probar su aplicación efectiva para cumplir los objetivos obligatorios de integridad y confidencialidad de la información personal.

La anterior Directiva 95/46/CE nos indicaba, al igual que nuestra vigente LOPD nos indica, de manera detallada los requisitos y obligaciones en el tratamiento de la información personal, a

---

102 En este sentido puede consultarse El Derecho.com (5 de enero de 2017). El Derecho a la Portabilidad no está limitado a los datos comunicados de manera directa por su titular (consultado el 18 de enero de 2017).

103 Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016, pp. 5 y 6).

104 En cuanto a la inscripción de ficheros en España puede consultarse la web de la AEPD (consultado el 27 de enero de 2017).

105 En relación con las medidas de seguridad en España puede consultarse la web AEPD (consultado el 17 de octubre de 2016). En todo caso, el principio de seguridad de datos (art. 9 LOPD) impone al responsable del fichero adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Estas medidas han sido desarrolladas en el Título VIII del RLOPD.

diferencia del RPD que deja más en nuestras manos decidir qué medidas implantamos, pero, eso sí, debiendo justificar nuestra elección y, ante todo, acreditar documentalmente su cumplimiento[106]. Se trata de la llamada responsabilidad proactiva[107].

5.1. Responsabilidad proactiva

El responsable o el encargado del tratamiento deberá aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RPD, por lo que se hace preciso la adopción de políticas de protección de datos que no solo han de existir, sino que han de estar adaptadas a las circunstancias de la organización, implementadas y funcionar en la práctica[108]. Se traslada una responsabilidad al responsable[109], pudiéndose demostrar el cumplimiento de las obligaciones de dos maneras diferentes: la adhesión a códigos de conducta o mediante un mecanismo de certificación[110].

A modo de ejemplo, antes una consulta pequeña de un dentista tenía que aplicar las mismas medidas de seguridad que un gran centro hospitalario, porque trataba datos personales referidos a la salud, a los que se les aplica medidas de nivel alto. Ahora, con el nuevo RPD, se discrimina el tipo de riesgo de cada centro, pues no es lo mismo, a nivel de estigmatización, un enfermo de sida que una persona que se arregla una caries[111].

5.2. Privacidad desde el diseño y por defecto

Con el objetivo de dar cumplimiento al principio de responsabilidad proactiva en materia de protección de datos, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el momento del diseño de sus procedimientos, productos y servicios (*privacy by design*), así como la obligación de que, por defecto, solo sean objeto de tratamiento los datos personales mínimos que sean necesarios para alcanzar el fin legítimo perseguido (*privacy by default*)[112].

106 Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016, p. 5).

107 Artículo 24 del RPD.

108 Piñar Mañas, J. L. (junio 2016, p. 28).

109 Cdos. 13 y 74 del RPD.

110 Cdo. 88 del RPD.

111 En este sentido, Lavanguardia.com (30 de septiembre de 2016).

112 Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016, p. 8).

Por lo tanto, la aplicación del principio de privacidad desde el diseño y del de privacidad por defecto exigen de los responsables una serie de implicaciones, que podríamos resumir en las siguientes[113]:

- Gestionar los mínimos datos posibles para alcanzar la finalidad establecida.
- Limitar los accesos a los datos, aplicando medidas proporcionales a la sensibilidad de los mismos.
- Proporcionar al titular de los datos los medios de control efectivo sobre los datos.
- Garantizar que en todo momento el interesado disponga de información suficiente y veraz sobre el tratamiento.
- Realizar evaluaciones de impacto, que serán obligatorias en los casos en los que el tratamiento entrañe un alto riesgo para los derechos de los titulares.

En el entorno actual la aplicación de estos principios supone un soplo de aire fresco para los ciudadanos, pues se va a reforzar la posición de los usuarios en el tratamiento de sus datos, así como en la preservación de su privacidad, a la par que se pretende la prestación de un servicio más seguro. Al hilo de lo dicho, cabe preguntarnos si hubiera sido necesario que el TJUE consagrara mediante sentencia el derecho al olvido, de haberse obligado a los buscadores como Google a aplicar los principios de privacidad por diseño y por defecto[114].

5.2.1. Privacidad desde el diseño

El RPD regula la privacidad desde el diseño[115] como elemento de necesario estudio antes de acometer cualquier proyecto tecnológico que implique tratamiento de datos. Así, los especialistas en protección de datos tendrán que estar más involucrados, si cabe, con los *developers* (desarrolladores, por ejemplo de *apps*) y otros profesionales en la fase de diseño de los proyectos, evitando de esta manera que los proyectos tecnológicos desarrollados por las empresas precisen modificaciones *a posteriori* en materia de privacidad[116].

A modo de ejemplo, para la privacidad desde el diseño un sistema, una *app*, serán plenamente funcionales (cualquiera que sea su objetivo, siempre que sea legítimo) y, a la vez, plenamente

---

113 En este sentido, UBT Compliance (UBTc): Reglamento europeo de protección de datos: ¿qué es la privacidad desde el diseño? (consultado el 17 de enero de 2017).

114 En este sentido, La Privacidad desde el Diseño y por Defecto. Disponible en <www.laleydeinternet.com> (consultado el 1 de marzo de 2017).

115 Cdo. 78 y artículo 25.1 del RPD.

116 En este sentido, La Privacidad desde el Diseño y por Defecto. Disponible en <www.laleydeinternet.com> (consultado el 7 de marzo de 2017).

respetuosos con la privacidad de sus usuarios, o no serán nada. No se trata de supeditar la utilidad a la privacidad, sino de diseñar y construir sistemas y prácticas en los que ambos principios se desarrollen plenamente. En definitiva, la tecnología no ha de ser una amenaza para la privacidad, así como la privacidad no ha de ser un obstáculo que frene el desarrollo de la tecnología[117].

5.2.2. Privacidad por defecto

No solo basta con diseñar una aplicación o un servicio web realizando un enfoque garantista en materia de protección de datos, sino que, además, por defecto el servicio debe garantizar el máximo grado de privacidad posible[118]. Esto implica que en materia de redes sociales los perfiles de privacidad de los usuarios estarán por defecto cerrados a otros usuarios, debiendo ser el usuario quien los abra a otros[119]. El responsable del tratamiento deberá aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación alcanza a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad[120].

Supongamos, a modo de ejemplo, la firma de un nuevo servicio de medios de comunicación social en el que se puede compartir información personal, acontecimientos de la vida y otros datos con terceros. Con el fin de publicar con éxito el perfil solo se requiere el nombre y dirección de correo electrónico, sin embargo, el nuevo servicio también publica automáticamente la edad y la localización, haciéndolo disponible al público en lugar de solo a sus conexiones. Esto sería una clara violación de la privacidad por defecto pues, en principio, se da a conocer al público más información de la necesaria para ofrecer el servicio, pues la opción de compartir datos con terceros debe encontrarse deshabilitada desde su origen, pudiendo solo activarse la opción de compartir datos con terceros mediante un acto expreso del usuario[121].

6. NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

La obligación de notificar las brechas de seguridad[122] en dispositivos que almacenan datos personales encuentra su justificación en el riesgo de daños y perjuicios para los consumidores y

---

117 Galindo Q. J. (julio-diciembre de 2014). Privacy by design. Implementing privacy as a good business decision. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, *12*, 4 a 24 (consultado el 31 de octubre de 2016).

118 En este sentido, *La Privacidad desde el Diseño y por Defecto* (consultado el 7 de marzo de 2017).

119 Carlos FH-Redacción Noticias Jurídicas (4 de mayo de 2016).

120 Cdo. 78 y artículo 25.2 del RPD.

121 En este sentido, EU Data Protection Regulation: Data Protection by Design and by Default (consultado el 31 de octubre de 2016).

122 Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016, p. 8).

usuarios[123], como es el caso de la pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización[124], daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión[125].

La obligación de notificar las incidencias de seguridad que impliquen una violación de datos personales que con la LOPD solo afectaba a las empresas de telecomunicaciones y a los proveedores de acceso a internet (ISP)[126], con el RPD se extiende a cualquier responsable del tratamiento, no limitándose exclusivamente a las empresas del sector de las comunicaciones electrónicas[127]. Si la brecha de seguridad afecta negativamente a la protección de los datos personales o a la privacidad del interesado, se debe informar tanto a la Agencia de Protección de Datos como al afectado[128]:

- Notificación a la autoridad de control: dentro de las 72 horas siguientes, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas[129].
- Notificación al interesado: sin dilación indebida, en caso de que pueda entrañar un alto riesgo para sus derechos y libertades, permitiéndole tomar las precauciones necesarias, que deberá realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales[130].

---

123 Viguri Cordero, J. A. (2016). La implementación de nuevos esquemas de certificación en la UE como garantía de los derechos fundamentales de consumidores y usuarios (especial referencia a la protección de datos personales). *Revista CESCO de Derecho de Consumo*, *19*, 31 (consultado el 12 de diciembre de 2016).

124 Seudonimización (art. 4.5 RPD): información que, sin incluir los datos denominativos de un sujeto afectado (es decir, aquellos que lo pueden identificar de manera directa), sí que potencialmente permiten, a través de la asociación con información adicional, determinar quién es el individuo que está detrás de los datos seudonimizados.

125 Cdos. 85 a 88 y artículos 33 y 34 del RPD.

126 ISP (*Internet service provider* o, en español, proveedor de servicios de internet) es un servicio (en la mayoría de los casos de pago) que permite conectarse a internet.

127 En este sentido, Brocca, M. (7 de marzo de 2017). Cómo gestionar las brechas de seguridad según el nuevo reglamento de protección de datos. *Security Art Work* (consultado el 9 de marzo de 2017).

128 Saiz Peña, C. A. (2015). La notificación de brechas de seguridad. En A. Rallo Lombarte y R. García Mahamut (Coords.): *Hacia un nuevo derecho europeo de protección de datos. Towards a new european data protection regime* (pp. 771 a 817). Tirant lo Blanch.

129 En este sentido, Autoridad Catalana de Protección de Datos. ¿Cuáles son las principales novedades del Reglamento General de Protección de Datos (RPD)? (consultado el 22 de octubre de 2016).

130 Palma Villalón, M. del V. (1 de mayo de 2016).

7. EVALUACIONES DE IMPACTO

La evaluación de impacto en protección de datos, si bien resulta una figura novedosa en nuestro país (o análisis de riesgos en privacidad)[131], lleva años implantada en el mundo anglosajón. A modo de ejemplo, en Estados Unidos resulta obligatoria para determinados tratamientos efectuados por agencias gubernamentales desde la *E-Govermment Act* de 2002. En Canadá, a nivel federal, existe obligación de efectuar evaluaciones de impacto para los entes públicos bajo la *Directive on Privacy Impact Assesment*. En otros casos, como el de Australia, pese a no tratarse de una obligación legal, las evaluaciones de impacto son promovidas por las agencias de protección de datos tanto para entes públicos como para organizaciones privadas[132].

Si bien la Directiva 95/46/CE y la LOPD establecieron la obligación de notificar los ficheros a la autoridad de control, dado que esta medida no ha contribuido a mejorar la protección de datos personales, el RPD la sustituye por la obligación de realizar una evaluación de impacto[133].

El desarrollo a nivel europeo de un marco unificado en relación con las evaluaciones de impacto en protección de datos (EIPD)[134] encuentra su razón de ser en el auge de nuevos modelos de negocio, comunicaciones y medios tecnológicos, tales como las tecnologías *wearables*[135], el auge del internet de las cosas[136] (IoT)[137], la progresiva implantación de soluciones de cruzamiento masivo de datos o *big data*, el procesamiento de datos sensibles de carácter religioso o ideológico, el tratamiento de datos biométricos, la geolocalización, las nuevas fronteras en el ámbito de la ciberseguridad, el *finger printing* o la tecnología de reconocimiento facial en redes sociales dan lugar a nuevos riesgos que pueden tener consecuencias con carácter simultáneo en distintas localizaciones[138].

---

131 Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016, p. 11).

132 En este sentido, Perez, J. L. (2016). Las Evaluaciones de Impacto en el Reglamento Europeo de Protección de Datos, *Blog Compliance-Ribas y Asociados* (consultado el 31 de octubre de 2016).

133 Palma Villalón, M. del V. (1 de mayo de 2016).

134 Cdos. 84, 90 a 95 y artículo 35 del RPD.

135 Dispositivos *wearables*; ¿Qué es *wearable*? – Los dispositivos vestibles. *Wearable* hace referencia al conjunto de aparatos y dispositivos electrónicos que se incorporan en alguna parte de nuestro cuerpo interactuando de forma continua con el usuario y con otros dispositivos con la finalidad de realizar alguna función concreta, como pueden ser relojes inteligentes o *smartwatchs*, zapatillas de deportes con GPS incorporado y pulseras que controlan nuestro estado de salud, disponible en <www.dispositivoswearables.net> (consultado el 2 de noviembre de 2016).

136 Viguri Cordero, J. A. (2016, p. 30).

137 Wikipedia: Internet de las cosas (en inglés, *Internet of things*, abreviado *IoT*) es un concepto que se refiere a la interconexión digital de objetos cotidianos con internet (consultado el 2 de noviembre de 2016).

138 Díaz, E. (2016). El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones. *Revista Aranzadi Doctrinal*, *6*, parte Estudio, apartado 2.7.2. Evaluación de impacto en la privacidad. Pamplona: Aranzadi. Westlaw BIB 2016\3067.

El responsable del tratamiento debe realizar una EIPD siempre que sea probable que las operaciones de tratamiento, especialmente cuando se utilicen nuevas tecnologías, entrañen un alto riesgo para los derechos y libertades de las personas físicas[139], que evalúe, en particular los siguientes conceptos: el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo[140].

Cuando una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación[141], debe consultarse a la autoridad de control antes del tratamiento[142].

La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos, podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos[143].

8. DELEGADO DE PROTECCIÓN DE DATOS

La designación del delegado de protección de datos[144] (DPO)[145] encuentra su fundamento en el artículo 18.2 de la Directiva 95/46/CE, que establecía la posibilidad de que los Estados miembros introdujesen esta figura en lugar de una obligación general de notificación[146].

En el nuevo marco de la protección de datos el DPO adquiere un protagonismo esencial[147], resultando obligatorio que sea designado, por el responsable y el encargado de tratamiento de datos, atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para ejecutar los cometidos contemplados en el RPD[148], en los siguientes casos[149]:

---

139 Piñar Mañas, J. L. (junio 2016, p. 28).

140 Cdo. 84 del RPD.

141 Aragonés Salvat, J. (5 de julio de 2016). La evaluación de impacto en el GDPR. Ateneu – Privacy Consulting (consultado el 31 de octubre de 2016).

142 Cdo. 94 del RPD.

143 Palma Villalón, M. del V. (1 de mayo de 2016).

144 Cdo. 97 y artículo 37 del RPD.

145 En inglés *data protection officer* (DPO).

146 En este sentido, La nueva figura del Delegado de Protección de Datos (7 de junio de 2013). En <www.delegadoprotecciondatos.com> (consultado el 2 de noviembre de 2016).

147 Piñar Mañas, J. L. (junio 2016, p. 28).

148 Díaz Díaz, E. (2016).

149 Artículo 37.1 del RPD.

- Cuando el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
- Cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieran una observación habitual y sistemática de interesados a gran escala.
- Cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales (datos de origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, biométricos, de salud o vida y orientación sexuales y datos relativos a condenas penales y delitos)[150].

Además cabe la posibilidad de que un grupo empresarial nombre un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento, así como que cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público se pueda designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño[151].

En cuanto a las funciones que tendrá el DPO[152], destacan el asesoramiento general dentro de la compañía en todo lo relativo a protección de datos personales, la supervisión del cumplimiento de la legislación y políticas de privacidad con especial atención a los riesgos asociados a las actividades que llevara a cabo la empresa, la elaboración de informes de evaluación de impacto de ciertos tratamientos de datos personales y la cooperación con las autoridades de control nacionales[153].

A la vista de las funciones del DPO se abre el debate sobre quién debe estar detrás de este perfil profesional que debe reunir determinadas capacitaciones y competencias[154]. ¿Debe diseñarse un nuevo perfil de abogado digital? Ya no solo hablamos del responsable de seguridad que se encargaba de hacer los avisos legales y de inscribir los ficheros, sino que estamos ante una figura relevante dentro del modelo de negocio de la empresa[155].

Se corre el peligro de que se convierta en una guerra entre profesionales con distintos perfiles: tecnólogos, informáticos, ingenieros, abogados,... y la imprecisión en la regulación va a provocar

150 Díaz Díaz, E. (2016).

151 Artículo 37.2 y 3 del RPD.

152 Palma Villalón, M. del V. (1 de mayo de 2016).

153 Artículo 39 del RPD, funciones que como mínimo tiene el delegado de protección de datos.

154 Cdo. 97 del RPD indica que «el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos».

155 Puede consultarse <www.ayudaleyprotecciondatos.es/2016/06/07/funciones-delegado-proteccion-datos/>.

tensiones si no se consigue tener una perspectiva global y conciliadora. Muchas dudas nos asaltan: ¿quién podrá ser DPO: un abogado con conocimientos tecnológicos o un técnico con conocimientos de Derecho? ¿Será preciso un «carnet profesional» que acredite los conocimientos? ¿Qué capacitación va a necesitar el DPO? ¿Se optará por un modelo similar a los requisitos exigidos para ser *mediador* con un número de horas formativas regulado y un perfil jurídico? ¿Quién definirá el perfil: el legislador en el desarrollo del RPD o la empresa, según las necesidades del mercado –autorregulación–? ¿Cómo evitar el intrusismo profesional y garantizar una calidad en los servicios? ¿Se optará por un esquema de certificación y acreditación de competencias? ¿Y cuál: ISO[156], ENAC[157], ISACA[158]...?

Si bien a los profesionales expertos en privacidad se les ha abierto la puerta a un mar de oportunidades –a la par que un sinfín de retos por superar–[159], parece ser que en el mes de abril de 2018, a un mes de la plena aplicación del 25 de mayo del RPD, el número de profesionales notificados a la AEPD es prácticamente insignificante –apenas varias decenas–[160].

9. TRANSFERENCIAS INTERNACIONALES DE DATOS

Las transferencias internacionales de datos, en el ordenamiento jurídico español[161], es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español[162].

Por su significativa incidencia en el nuevo RPD y especial trascendencia en este ámbito hemos de hacernos eco de la Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de

156 Organización Internacional de Normalización (en inglés, International Organization for Standardization, conocida por ISO) es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización, sitio oficial <www.iso.org> (consultado el 14 de diciembre de 2016).

157 Entidad Nacional de Acreditación (ENAC) declarada, según el Real Decreto 1715 de 2010 del Estado español, como el único organismo dotado de potestad pública para otorgar acreditaciones de acuerdo con lo establecido en el Reglamento Europeo (CE) núm. 765/2008, sitio oficial <www.enac.es> (consultado el 14 de diciembre de 2016).

158 ISACA, acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información, sitio oficial <www.isaca.org> (consultado el 14 de diciembre de 2016).

159 Carlos FH-Redacción Noticias Jurídicas (28 de enero de 2016). Los retos de la protección de datos en 2016 (consultado el 15 de diciembre de 2016).

160 En este sentido puede consultarse la web de Cinco Días: La Agencia Española de Protección de Datos habilita un canal para comunicar el «DPO» (consultado el 15 de abril de 2018).

161 Artículos 33 y 34 de la LOPD y título VI del RLOPD.

162 En este sentido puede consultarse la web de la AEPD (consultado el 12 de diciembre de 2016).

2015 (petición de decisión prejudicial planteada por la High Court-Irlanda) –Maximillian Schrems / Data Protection Commissioner–[163], por significar un punto de inflexión respecto a cómo se venían realizando las transferencias internacionales de datos de empresas desde la UE a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales en el sentido de que no debe menoscabar el nivel de protección de las personas físicas garantizado en la UE por el nuevo RPD, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional[164].

Con este objetivo de garantizar el nivel de protección a los interesados se refuerza el régimen de transferencias internacionales de datos[165], por lo que en ausencia de una decisión por la que se constate la adecuación de la protección de los datos[166], el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado[167].

Así, a modo de ejemplo, indicar que no será suficiente para autorizar una transferencia de un servicio de alojamiento de documentos en la nube que el proveedor afirme ser seguro, sino que se precisará que acredite que ha implementado las medidas de seguridad oportunas y que, en caso de efectuar sucesivas transferencias internacionales de datos a otros proveedores, también estos adoptan las garantías tecnológicas suficientes.

10. RÉGIMEN SANCIONADOR

Las autoridades de control nacionales, como la AEPD, que tienen asignados poderes correctivos y conservan importantes competencias como las de inspección (actual auditoría) y, como

163 STJUE de 6 de octubre de 2015, Asunto C-362/14 (NCJ060337), puede consultarse en <www.curia.europa.eu> (consultado el 12 de febrero de 2016). El TJUE estima que la existencia de una Decisión de la Comisión que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la Unión Europea y de la Directiva.

164 Freije Trapiella, B. (21 de febrero de 2017). Las transferencias internacionales de datos personales y el reto de salvaguardar los derechos fundamentales de los afectados. *ElDerecho.com* (consultado el 14 de marzo de 2017).

165 Artículos 44 a 50 del RPD.

166 Artículo 45 del RPD. Transferencias basadas en una decisión de adecuación: cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de este país o la organización internacional garantizan un nivel de protección adecuado.

167 Artículo 46 del RPD. Transferencias mediante garantías adecuadas: que podrán reflejarse, entre otros, en un instrumento jurídicamente vinculante, normas corporativas vinculantes, cláusulas tipo de protección de datos, mecanismos de certificación, cláusulas contractuales o códigos de consulta.

no, las de sanción a presuntos infractores, son las garantes independientes del cumplimiento del RPD, coordinadas ahora bajo el paraguas del llamado Comité Europeo de Protección de Datos, que facilita su coordinación y coherencia a nivel internacional[168].

Los poderes correctivos otorgados a las autoridades nacionales consisten en sancionar con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el RPD, sancionar con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el RPD, ordenar que se atiendan las solicitudes de ejercicio de los derechos del interesado, ordenar que las operaciones de tratamiento se ajusten al RPD, así como que se comunique al interesado las violaciones de la seguridad de los datos personales[169].

En relación con las competencias de sanción advertir que el RPD sobresale por su potencial dureza en las multas administrativas, las cuales, si bien deben ser «efectivas, proporcionadas y disuasorias»[170], podrán alcanzar, según los casos, hasta los 10 millones de euros o el 2% del volumen de facturación[171], o hasta los 20 millones de euros o el 4% del volumen total de negocio[172], optándose en ambos casos por el importe que resulte mayor. Esta dureza en las multas administrativas pone en el punto de mira en las grandes compañías de telecomunicaciones o de internet, que no se veían muy afectadas potencialmente por el anterior régimen sancionador, si bien en España podían alcanzar los 600.000 euros[173]. En todo caso, a más tardar para el 25 de mayo de 2018, se contempla la posibilidad que los Estados miembros comuniquen a la Comisión otras sanciones que decidan aplicar para las infracciones que no estén sancionadas con multas administrativas en el RPD[174].

11. AUTORREGULACIÓN Y CERTIFICACIÓN

El RPD apuesta por el impulso a la autorregulación mediante la creación de códigos de conducta, así como por el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, hasta el punto de que la adhesión a códigos de conducta o a algún mecanismo de certificación podrá utilizarse como elemento probatorio del cumplimiento de las obligaciones por parte del responsable del tratamiento[175].

---

168 Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016, p. 9).

169 Artículo 58.2 del RPD.

170 Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016, p. 9).

171 Artículo 83.4 del RPD.

172 Artículo 83.5 del RPD.

173 Artículo 45.3 de la LOPD, las infracciones muy graves son sancionadas con multas de hasta 600.000 euros.

174 Artículo 84 del RPD.

175 Artículo 24.3 del RPD.

11.1. Autorregulación

En cuanto a la autorregulación señalar que desde el ámbito institucional se contempla que los Estados miembros promoverán la elaboración de códigos de conducta específicos, según los sectores de tratamiento, que tendrán en cuenta las necesidades particulares de microempresas y las pequeñas y medianas empresas[176]. Igualmente se prevé que las asociaciones y organismos representativos de categorías de responsables o encargados del tratamiento, a los que resulte de aplicación el RPD, podrán también elaborar códigos de conducta, modificar o ampliar los ya existentes[177], debiendo presentar el proyecto de código de la modificación o ampliación a la autoridad de control competente[178]. Los responsables o encargados no vinculados por las disposiciones del RPD podrán igualmente adherirse a estos códigos, en las circunstancias y en los casos previstos, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales[179].

A los efectos de favorecer la autorregulación y los códigos de conducta en la aplicación del RPD, tal vez sea conveniente, por un lado, en el ámbito de la empresa, plantear la posibilidad de acudir al arbitraje en materia de protección de datos, evitando en lo posible el recurso directo a la denuncia ante la AEPD, incluyendo, en su caso, una posible oferta de indemnización al usuario que prescinda de la denuncia y la posterior sanción; y, por otro lado, en un ámbito sectorial, favorecer la autorregulación, de forma que al menos los principales sectores de actividad establezcan sus propios requerimientos específicos y homogéneos. Por último también cabría plantearse la conveniencia de la autorregulación a nivel de las autoridades de control[180].

11.2. Certificación

A los efectos de aumentar la transparencia y el cumplimiento del RPD, se fomenta el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan, por un lado, a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes; y permitan, de otro lado, a los responsables y encargados del tratamiento demostrar el cumplimiento del RPD[181].

---

176 Artículo 40.1 del RPD.

177 Artículo 40.2 del RPD.

178 Cdos. 98 y 99 del RPD.

179 Artículo 40.3 del RPD.

180 Carlos FH-Redacción Noticias Jurídicas (30 de abril de 2016). El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre nuevas perspectivas profesionales a la abogacía (consultado el 12 de diciembre de 2016).

181 Artículos 42 y 43 y Cdo. 100 del RPD.

El proceso de certificación es voluntario y deberá siempre ser transparente[182], por lo que los responsables o encargados que sometan su tratamiento al mecanismo de certificación deberán facilitar al organismo de certificación toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación[183]. Los mecanismos de certificación podrán ser expedidos por los organismos de certificación, la autoridad de control competente o el Comité Europeo de Protección de Datos, facultado a este último la posibilidad de crear una única certificación común, el denominado «sello europeo de protección de datos»[184].

En interés del efectivo control de todo el proceso de certificación, la certificación se expide por un plazo máximo de tres años, si bien podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes[185]. Cabe entender que lo que se pretende es establecer una cautela al uso prolongado del mecanismo de certificación mediante un nuevo examen en un plazo máximo de tres años. Sin embargo, no se contempla la posibilidad de que en este plazo de tres años se modifiquen las condiciones de la certificación ante nuevos retos que requieran de condiciones más exigentes.

En todo caso indicar que el RPD regula lo referente a los mecanismos de certificación centrándose en los múltiples beneficios que presenta, pues son instrumentos enormemente flexibles que pueden adaptarse rápidamente a los cambios continuos de la sociedad y, además, se adecúan mejor a un sector determinado, elevando notoriamente su nivel de protección[186].

IV. EN ESPECIAL, LA CERTIFICACIÓN

En los últimos años estamos viviendo una auténtica revolución tecnológica, con un incremento diario exponencial de datos. El flujo de información es continuo, masivo y además global. Navegamos por internet y dejamos un rastro digital continuo, como puede ser, a modo de ejemplo, cuando realizamos búsquedas, compramos *online*, descargamos aplicaciones, participamos en redes sociales, subimos fotos o hacemos uso de servicios de mensajería instantánea. Los sitios que frecuentamos están geolocalizados. Cada vez los detalles son más íntimos, compartimos nuestros estados de ánimo o intereses de manera inconsciente, todo ello debido a la poca cultura digital y la falacia de la gratuidad y el anonimato[187].

182 Artículo 42.3 del RPD.

183 Véase artículo 42.6 del RPD.

184 Artículo 42.5 del RPD y Miralles R. Sello Europeo de Protección de Datos. *Abogacía Española* (consultado el 8 de enero de 2017).

185 Véase artículo 42.7 del RPD.

186 Véase artículo 42 del RPD.

187 Asociación Profesional Española de Privacidad. (Enero 2015). Revolución tecnológica, social y cambios legales en protección de datos. Los grandes retos a la privacidad (consultado el 5 de septiembre de 2016).

Si bien, por un lado, los novedosos productos de seguridad ofrecen una serie de ventajas incuestionables para los consumidores y usuarios, no es menos cierto que, por otro lado, presentan una serie de retos potenciales pues son susceptibles, no solamente de generar fallos en seguridad y eficiencia, sino que, a su vez, afectan directamente en los derechos fundamentales de los consumidores y usuarios[188].

Si bien con la certificación se pretende solventar todos estos conflictos, no es menos cierto que la falta de armonización a nivel europeo de los esquemas de certificación supone un problema de enorme calado en la actualidad, pues cada Estado miembro aplica determinadas normas técnicas que requieren de recertificación conforme a diferentes estándares en otro Estado miembro, dificultándose en este sentido la libre circulación de mercancías, la primera de las cuatro libertades fundamentales del mercado interior[189].

1. HOMOGENEIZACIÓN

Las organizaciones que se someten a sistemas de certificación disfrutan de una ventaja competitiva significativa, puesto que basan sus procesos en el examen por parte de un tercero imparcial que controla la adecuación del producto a determinados estándares[190], lo que posibilita que sean adaptados de un modo eficiente a los requisitos que demandan los consumidores y usuarios. Ahora bien, el desarrollo imparable de las nuevas tecnologías hace evidente la necesidad de superar la certificación que se base en la creación de normas estancas, así como la necesidad de creación de nuevos esquemas de certificación que ya no solo incorporen aspectos básicos en materia de seguridad o eficiencia, sino también otras dimensiones que afectan directamente a los consumidores y usuarios[191], para así aumentar la transparencia y la continua adaptación a necesidades y exigencias técnicas, jurídicas y legales[192]. En este sentido podemos mencionar una iniciativa innovadora a nivel europeo: el proyecto CRISP[193] (evaluación y certi-

188 Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. En III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas. *IDP*, *Revista de Internet, Derecho y Política*, *5*, 47 a 61 (consultado el 19 de diciembre de 2016).

189 Artículos 26 y 28 al 37 del TFUE, disponible en <www.eur-lex.europa.eu> (consultado el 20 de diciembre de 2016).

190 Como puede ser, a título de ejemplo, la seguridad, la eficiencia o mediante la garantía de unas condiciones más favorables que las establecidas en la ley.

191 En este sentido, Grupo de Trabajo del Artículo 29 (9 de enero de 2009). Opinión 1/2007 relativo al Libro Verde sobre las tecnologías de detección en la labor de los servicios represivos, aduaneros y otros servicios públicos de seguridad. *WP129* (consultado el 12 de diciembre de 2016).

192 Viguri Cordero, J. A. (2016, p. 34).

193 CRISP (Evaluation and Certification Schemes for Security Products) es un proyecto europeo (abril 2014/marzo 2017) financiado por el 7.º Programa Marco de la Unión Europea para la investigación y desarrollo tecnológico, puede consultarse en <www.crispproject.eu> (consultado el 14 de diciembre de 2016).

ficación de esquemas para productos de seguridad), que surge como una iniciativa puntera que persigue el objetivo de desarrollar una novedosa metodología de evaluación para la certificación de productos, servicios y sistemas de seguridad integrando dimensiones sociales como la seguridad, la confianza, la eficiencia y la prevención en la violación de derechos fundamentales como criterios de evaluación[194].

Con objeto de solventar los problemas anteriormente mencionados, la Comisión Europea ha priorizado en la implementación de esquemas de certificación homogéneos en toda la UE que incorporen un conjunto de normas técnicas y legales que garanticen un alto nivel de protección para los consumidores y usuarios[195]. Además, con la adopción de nuevos esquemas de certificación los productos resultarán más competitivos, pues la homogeneización comportará una reducción de los costes de producción, al ser diseñados desde un principio siguiendo unas pautas claras conforme a determinadas normativas revirtiendo, asimismo, en un sustancial ahorro económico para el consumidor final.

2. PREVENCIÓN

Las organizaciones que tratan con datos personales poseen una responsabilidad activa en su tratamiento, por lo que deben adoptar medidas de prevención efectivas que aseguren el cumplimiento de los derechos, garantías y principios establecidos en el RPD, pues una vez producida la infracción (como deja entrever el propio RPD), las organizaciones ya no pueden actuar, debido a que pueden causar daños de muy difícil o imposible reparación a los consumidores y usuarios.

Tal vez la necesidad de adoptar medidas de prevención efectivas, junto con la posibilidad de que la normativa no pueda actualizarse y adaptarse eficientemente a los nuevos cambios tecnológicos que se producen en nuestra sociedad[196], es por lo que el RPD enfatiza la promoción de esquemas de certificación. En todo caso advertir que también promueve códigos de conducta, al igual que un conjunto de medidas tendentes a prevenir los quebrantos en la privacidad y protección de datos, tales como: la protección de datos desde el diseño, la protección de datos por de-

194 El Proyecto CRISP ha incorporado a destacadas organizaciones de consumidores y usuarios de los Estados miembros así como a asociaciones de consumidores a nivel europeo como European Digital Rights (EDRI) o The European Consumer Organisation (BEUC) para compartir su experiencia en la redefinición de la metodología de CRISP.

195 Comisión Europea. *Una visión estratégica de las normas europeas: Avanzar para mejorar y acelerar el crecimiento sostenible de la economía europea de aquí a 2020.* Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, COM (2011)311 final, Bruselas, junio 2011, en <www.eur-lex.europa.eu> (consultado el 20 de diciembre de 2016).

196 En este sentido, Sección 5, relativa a «Códigos de conducta y certificación», capítulo IV rubricado «Responsable del tratamiento y encargado del tratamiento», artículos 40 y ss. del RPD.

fecto, las medidas de seguridad, el mantenimiento de un registro de tratamientos, la realización de evaluaciones de impacto sobre la protección de datos, el nombramiento de un delegado de protección de datos y la notificación de violaciones de la seguridad de los datos.

Si bien no cabe duda de que el RPD apuesta claramente por la certificación como instrumento de prevención y adaptación a los cambios tecnológicos, conviene destacar que si bien la actualización de los requisitos técnicos que ya están en el mercado (objeto de certificación hasta la fecha) debe llevarse a cabo de forma que estos se adapten de un modo ágil y dinámico a los continuos cambios tecnológicos, resulta cada vez más necesario la incorporación o adhesión de dimensiones legales (e incluso sociales) al esquema de certificación de modo que se otorgue un verdadero valor añadido al sello o marca final, protegiendo de forma efectiva los derechos de los consumidores y, usuarios y, por ende, aumentando la confianza de la sociedad en estos mecanismos.

V. A MODO DE CONCLUSIÓN

Si bien internet y las nuevas tecnologías permiten nuevas posibilidades de comunicación, que unos años atrás nos podían parecer utópicas, simultáneamente surgen nuevos riesgos. Las nuevas posibilidades de acumulación de datos y de elaboración de perfiles comportan una mayor capacidad de control sobre los individuos, que en ocasiones puede darnos la sensación de «desnudez» de nuestra vida privada.

Los avances técnicos en internet y las nuevas tecnologías deben ir en paralelo con la transparencia y con el respeto a los principios de protección de datos, por lo que la normativa debe tener por objeto proteger a las personas frente a las grandes corporaciones y compañías que almacenan y negocian con los datos de las personas, como pueden ser: ideología política, orientación sexual, salud y pautas de consumo, entre otros. En este sentido compete al legislador lograr un óptimo equilibrio entre la salvaguardia de la vida privada y el interés progresivo que tiene la sociedad en el tráfico de la información sobre las personas, información que se ha convertido en una mercancía muy valiosa.

En materia de protección de datos la aprobación del RPD ha supuesto la introducción de importantes novedades, desplegando aspectos muy relevantes y positivos, entre los que podemos indicar los siguientes:

- Se pone fin a la disparidad normativa al implantarse un marco legal sólido y uniforme de alcance europeo que permitirá salvaguardar el derecho fundamental a la protección de datos de los ciudadanos europeos o residentes en Europa, con la consiguiente seguridad jurídica y transparencia, a la par que fomentar la innovación, la creación de empleo, la generación de riqueza y liberar el potencial del mercado digital.

- Se amplía de forma considerable, desde un punto de vista subjetivo y territorial, el ámbito de protección en materia de protección de datos para los ciudadanos que forman parte de los Estados miembros de la UE, pues regula no solamente la protección de los datos personales de las personas físicas, sino también la circulación de esos datos, tanto en el ámbito territorial de la propia UE como en lo referente al tratamiento de los datos de los ciudadanos europeos fuera del ámbito de la UE.
- Estimulará la cooperación entre asociaciones de profesionales para defender la calidad del profesional en la privacidad y ocupar un lugar en el desarrollo del RPD.
- Se reivindica la figura del abogado digital, del jurista experto en privacidad, para que el pequeño empresario tenga una mejor comprensión de las obligaciones que establece el RPD.
- Estimulará la cooperación entre los actores del tratamiento y la gestión de los datos personales: empresas, Administraciones públicas, agencias de control, asesores y ciudadanos.

Por otra parte, podemos apreciar algunas sombras o amenazas en la nueva normativa europea de protección de datos, entre los que podemos mencionar las siguientes:

- Se trata de una norma muy técnica, extensa y minuciosa, resultado de una larga y compleja tramitación, que contiene numerosos conceptos jurídicos indeterminados en su articulado que dificultan su comprensión y que pueden generar problemas interpretativos en el futuro.
- Mientras no se avance en la cultura de la privacidad, el usuario no recuperará realmente el control de sus datos. Si bien se establece que el consentimiento para el tratamiento de datos ha de ser expreso, nada garantiza que el usuario sea verdaderamente consciente de lo que autoriza.
- Se olvida de la regulación jurídica de cuestiones tecnológicas actualmente operativas y de uso masivo por los ciudadanos, que tienen una incidencia directa en los datos personales: internet de las cosas, realidad virtual, *big data* o *cloud computing*.
- Si bien la normativa en materia de cumplimiento afecta a todos los entornos de la actividad, sin embargo da la impresión de que está pensada primordialmente para las grandes compañías, cuando la pequeña y mediana empresa es la más abundante, tanto a nivel europeo como nacional.
- Se establecen medidas aisladas y desordenadas para que el interesado pueda defender su derecho a la protección de datos, por lo que no existe una efectivo instrumento de ayuda al interesado para defender su derecho.

Y pese a que el RPD supone la derogación expresa de la Directiva 95/46/CE, no está derogada en cambio la normativa española de protección de datos, por lo que la pervivencia de estas dos normas suscita dudas acerca de su convivencia en materias tales como la obligatoriedad o no de seguir inscribiendo los ficheros, el papel que tiene que desempeñar la AEPD, etc., por lo que resultará importante ver la posición al respecto que se mantiene por la AEPD.

En todo caso las empresas disponen de un periodo transitorio de casi dos años para ir adecuando de manera progresiva sus procesos internos a los requisitos del RPD, adaptando las medidas jurídicas, técnicas y organizativas, de modo que cuando llegue la fecha de su efectiva aplicación, las empresas hayan culminado el proceso progresivo de adecuación y hayan implementado de manera efectiva los aspectos que garanticen el cumplimiento de la nueva regulación europea en materia de protección de datos.

VI. EPÍLOGO

Subrayar que es trascendental que los ciudadanos tomemos conciencia del grave peligro que asumimos al compartir nuestros datos personales de manera libre y sin protección, en especial porque pueden verse sometidos a decisiones que escapan a nuestro control y decisión.

Referencias bibliográficas

Aberasturi Gorriño, U. (2013). El derecho a la indemnización en el artículo 19 de la ley orgánica de protección de datos de carácter personal. *Revista Aragonesa de Administración Pública*, *41-42*, 173-206 Zaragoza.

Álvarez Hernando, J. y Cazurro Barahona, V. (2014). Ejercicio de derechos de acceso, rectificación, cancelación y oposición (arco). Derecho al olvido en internet. Westlaw BIB 2014\8354.

Arroyo Yanes, L. M. (1993). El Derecho de Autodeterminación Informativa frente a las Administraciones Públicas (Comentario a la STC 254/93, de 20 de julio). *Revista Andaluza de Administración Pública*, *16*, 119-240.

De Carreras Serra, Ll. (1996). *Régimen jurídico de la información. Periodistas y medios de comunicación*. Barcelona: Ariel Derecho.

De Miguel Asensio, P. A. (2012). Buscadores de Internet y protección de datos: La cuestión prejudicial de la Audiencia Nacional sobre Google. *La Ley*, *7.870*, 1-3.

De Miguel Asensio, P. A. (2015). Aspectos internacionales de la protección de datos: Las sentencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley Unión Europea*, 1-10.

Díaz, E. (2014). Los ciudadanos ante el «derecho al olvido. *Actualidad Jurídica Aranzadi*, *886*. Westlaw BIB 2014\1763.

Díaz, E. (2016). El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones. *Revista Aranzadi Doctrinal*, *6*. Westlaw BIB 2016\3067.

Galindo, Q. J. (2014). Privacy by design. Implementing privacy as a good business decisión. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, *12*, 4-24.

González Murúa, A. R. (1994). Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales. *Revista Vasca de Administración Pública*, *37*, 227-270.

Heredero Higueras, M. (1983). La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983. *Documentación Administrativa*, *198*, 139-158.

Lucas Murillo de la Cueva, P. (abril-junio 1999). La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos (Nueva Época)*, *104*, 35-60.

Lucas Murillo de la Cueva, P. (2003). La primera jurisprudencia sobre el derecho a la autodeterminación informativa. *Datospersonales.org: La Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, *1*.

Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. En III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas. *IDP*, *Revista de Internet, Derecho y Política*, *5*, 47-61.

Morais Gallego, J. P. (marzo 2006). Las nuevas tecnologías de la información y de la comunicación. Implicaciones legales. *Revista Galega do Ensino*, *48*, 431-449.

Moya Izquierdo, S. y Crespo Vitorique, I. (2014). Los motores de búsqueda y el «derecho al olvido» cuando la tecnología avanza más rápido que el Derecho. *Unión Europea Aranzadi*, *10*, 27-37.

Ordóñez Solís, D. (2011). *Privacidad y protección judicial de los datos personales*. Bosh.

Pérez Luño, A. E. (1989). Libertad informática y derecho a la autodeterminación informativa. *I Congreso sobre Derecho Informático* (p. 359 a 375). Universidad de Zaragoza.

Pérez Luño, A. E. (1996). *Manual de informática y derecho*. Barcelona: Ariel.

Piñar Mañas, J. L. (2009). Protección de Datos: origen, situación actual y retos de futuro. En P. Lucas Murillo de la Cueva y J. L. Piñar Mañas, *El Derecho a la Autodeterminación Informativa.* Madrid: Fundación Coloquio Jurídico Europeo.

Piñar Mañas, J. L. (junio 2016). Reglamento europeo de protección de datos: retos y oportunidades para la abogacía. *Revista del Consejo General de la Abogacía*, *98*, 26 a 29.

Rallo Lombarte, A. (2011). La privacidad en la era digital: El derecho al olvido. *Actualidad Jurídica Aranzadi*, *815*. Westlaw BIB 2011\273.

Rallo Lombarte, A. (2014). La garantía del «derecho al olvido» en internet. *Actualidad Jurídica Aranzadi*, *886*. Westlaw BIB 2014\1761.

Rivas López, J. L. y Salgado Seguín, V. (noviembre 2016). Hacia la seguridad de los datos después del Reglamento Europeo. *Jornadas Técnicas de RedIRIS 2016*.

Roldán Aguirre, I. (2016). Criterios del «derecho al olvido» en los buscadores de internet. *Revista Aranzadi Doctrinal*, *6*. Westlaw BIB 2016\3059.

Rubio Torrano, E. (2016). El derecho al olvido digital. *Revista Doctrinal Aranzadi Civil-Mercantil*, *1*. Westlaw BIB 2015\18280.

Saiz Peña, C. A. (2015). La notificación de brechas de seguridad. En A. Rallo Lombarte y R. García Mahamut (Coords.), *Hacia un nuevo derecho europeo de protección de datos. Towards a new European data protection regime* (pp. 771-817). Tirant lo Blanch.

Villaverde Menéndez, I. (mayo-agosto, 1994). Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993. *Revista Española de Derecho Constitucional*, *1*, 187 a 224.