Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

Editoriale

Los desafíos del Reglamento General de Protección de Datos y la adaptación de las legislaciones nacionales

di Rosario García Mahamut *

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46 (en adelante, RGPD), es norma directamente aplicable desde el 25 de mayo de 2018 (art. 99.2 RGPD), tiene alcance general y es obligatorio en todos sus elementos en virtud de lo dispuesto en el art. 288 del Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE).

* Catedrática de Derecho Constitucional. Universitat Jaume I. Investigadora Principal del proyecto de investigación concedido por el Ministerio de Economía y Competitividad y que lleva por título «El impacto del nuevo Reglamento Europeo de Protección de Datos: análisis nacional y comparado» (DER 2015-63635-R).

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

Editoriale

Como es sabido, más que una mera actualización normativa, el RGPD constituye una revisión de las bases legales del modelo europeo del derecho a la protección de las personas físicas respecto del tratamiento de datos de carácter personal que se adopta al amparo del derecho fundamental a la protección de los datos de carácter personal reconocido en el art. 8 de la Carta de los Derechos Fundamentales de la UE y en el art. 16 del TFUE.

El RGPD, con sus luces y sus sombras, da un paso al frente y decidido en aras de garantizar y fortalecer el derecho a la protección de los datos personales. Sin duda, la incorporación de nuevos derechos en una sociedad digitalizada y el perfeccionamiento de un sistema de garantías que extiende sus fronteras más allá de la UE constituye, en sí mismo, una decidida apuesta por fortalecer los derechos individuales y hacer frente a los retos que la vertiginosa evolución tecnológica y la globalización plantean al derecho a la protección de los datos personales y a la libre circulación de los mismos.

Obsérvese que, como bien expresa el considerando sexto del RGPD, la tecnología no solo permite que tanto las empresas privadas como las autoridades públicas a la hora de realizar sus actividades utilicen datos personales en una escala sin precedentes, sino que, también, las personas físicas difundan un volumen cada vez mayor de información personal a escala mundial. Internet y las actividades en línea lejos de circunscribirse a un ámbito territorial constituye una realidad ubicua y omnipresente.

Pues bien, si la tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de los datos personales dentro de la UE y la transferencia a terceros países y

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

organizaciones internacionales, se debe garantizar al mismo tiempo un elevado nivel de protección de los mismos.

El RGPD responde a la necesidad de ofrecer un marco sólido a través del cual se garantizara un nivel uniforme coherente y elevado de protección de las personas físicas en relación con el tratamiento de los datos personales en la UE que evitase las divergencias que dificultaran la libre circulación de datos personales dentro del mercado interior. Un reglamento que, en palabras del considerando 13, "proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros (…)».

Efectivamente, el reglamento pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora que perseguía la Directiva 95/46 cuya transposición por los distintos Estados condujo a un tratamiento fragmentado que acarreó diferencias ostensibles en el nivel de protección de los datos de carácter personal entre los distintos Estados miembros. Por ello, no debe soslayarse que el epicentro de ese objeto homogeneizador que persigue el reglamento –cuando diseña e incorpora un conjunto de novedades que afectan al contenido del derecho a la protección de los datos personales y a su sistema de garantías– se halla, en buena parte, en impedir que una aplicación

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

fragmentada de la normativa en los distintos Estados miembros genere una percepción generalizada en la opinión pública de que existen graves riesgos para la protección de las personas físicas, en particular en relación con las actividades en línea y, en consecuencia, tales diferencias puedan constituir «(...) un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión>>.

A pesar de que el reglamento es una norma de alcance general, obligatoria en todos sus elementos y directamente aplicable, lo cierto es que contiene 56 remisiones de diverso alcance que permite a los Estados, utilizando expresión del Consejo de Estado español, adaptar su regulación en distintos casos, al contexto nacional, o a fijar exenciones, derogaciones o condiciones específicas para determinadas categorías de tratamiento de datos, e incluso, en algunos supuestos el reglamento confiere carácter preceptivo a esa labor normativa de desarrollo.

Por ello, a mi juicio, el mayor de los desafíos jurídicos a los que se enfrenta la UE con la europeización del derecho fundamental a la protección de datos y ese propósito uniformador de enfoque global que se concreta en el RGPD es susceptible de ser abordado en tres planos interconectados.

En primer lugar, el RGPD incorpora materialmente novedades de calado que exige no solo su aplicación directa, desarrollo normativo, plena coordinación y cooperación entre los Estados miembros para dotar de efectividad y eficiencia el sistema de garantías diseñado, sino que, además, ello debe colegirse con las exigencias derivadas de un reglamento que contiene un gran número de habilitaciones para los

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

Editoriale

Estados, en el que abundan conceptos jurídicos indeterminados y cuyos considerandos exceden, en ocasiones, su papel habitual al ser remitidos frecuentemente por el articulado. De este modo, se producen desajustes de entidad entre las previsiones de un preámbulo con vocación normativa y el articulado. Ello generará conflictos que demandarán respuestas jurídicas por parte de los distintos operadores jurídicos y muy especialmente del TJUE.

De forma somera, recordemos que, entre otras novedades, el reglamento prevé: la incorporación de nuevos derechos; la ampliación del ámbito de aplicación territorial del Reglamento –este se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no–; la incorporación de toda una serie de medidas que conecta con lo que se conoce como responsabilidad activa y que afecta al sistema de prevención por parte de las organizaciones que tratan los datos y que van desde la determinación de las obligaciones del responsable y encargado del tratamiento (incluidas la adopción de medidas técnicas y organizativas –protección de datos desde el diseño y por defecto–) a la obligación de designar un delegado de protección de datos en determinados supuestos así como su posición y distintas funciones que deben desempeñar, destacando, entre otras, la de cooperar con la autoridad de control. En este ámbito, cobran especial relevancia los mecanismos de autorregulación (códigos de conducta, certificación, así como la previsión de supervisión de los mismos y el papel activo de los organismos de certificación); el especial tratamiento en las transferencias de datos personales a terceros países u organizaciones internacionales; la

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

regulación de las autoridades de control independientes, la competencia de la autoridad de control principal y sus funciones, el régimen de cooperación entre la autoridad de control principal y las demás autoridades de control interesadas así como la asistencia mutuas, operaciones conjuntas de las autoridades de control y los mecanismos de coherencia. En línea con lo anterior, se crea el Comité Europeo de Protección de Datos; se regulan los procedimientos que se adecúan al modelo establecido de ventanilla única al existir una autoridad de control principal y otras autoridades interesadas; se prevé una serie de disposiciones relativas a situaciones específicas de tratamiento e introduce un innovador régimen sancionador, entre otras muchas novedades.

En segundo lugar, los Estados miembros deben aplicar una norma que no necesita de incorporación mediante otra norma de naturaleza interna que tienda a limitar la intervención de los Estados, en principio, a la aplicación material de norma europea, sin perjuicio de la labor de depuración normativa y de los eventuales desarrollos de los que aquella pueda ser objeto.

La depuración del ordenamiento interno, como ha puesto de relieve el Consejo de Estado español[1], implica, entre otras acciones, la derogación de las normas nacionales que sean incompatibles con el

[1] Dictamen del Consejo de Estado, de 26 de octubre de 2017, relativo al anteproyecto de ley orgánica de protección de datos de carácter personal (BOE, Documento CE-D-2017-757).

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

mismo –y ello debe realizarse a través de disposiciones que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse–, así como eliminar cuantas disposiciones puedan resultar redundantes como consecuencia del efecto directo de aquél en la medida que pueden poner en cuestión la aplicación directa del Reglamento, siguiendo la jurisprudencia del Tribunal de Justicia de la Unión. Evidentemente, los Estados miembros tienen la obligación de hacer cuanto sea necesario para asegurar el efecto útil del conjunto de las disposiciones del Reglamento.

En tercer término, los Estados deben desarrollar aspectos novedosos claves de bóveda del sistema de garantías establecidos en el RGPD adecuando su normativa interna tanto al margen de discrecionalidad que éste les ofrece como a las limitaciones que el reglamento les impone con lo que ello acarrea desde el punto de vista interno para los Estados de revisión de su ordenamiento, derogaciones, implementación y sistematización normativa interna.

Los desafíos que introduce el reglamento son múltiples, tanto desde una perspectiva formal como sustantiva, y los distintos Estados miembros han adaptado y/o siguen adaptando sus legislaciones; y, ello, a pesar de que han contado con dos años para adaptar sus respectivas normas.

Pero a más, el RGPD es una norma que reviste no solo gran complejidad sino que su regulación se completa con la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

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. No en vano algunos de los ordenamientos que han adaptado su normativa al RGPD también han implementado la Directiva (UE) 2016/680.

Los distintos Estados miembros han adoptado técnicas diversas para adaptar su normativa al Reglamento y han optado, bien por modificar su legislación, bien por aprobar nuevas normas de protección de datos. En ambos supuestos también nos encontramos con algunos ordenamientos que han implementado la Directiva 2016/680 y otros que no.

En el primer supuesto, destacan, entre otros, Francia, Austria e Italia. Francia, modificó ampliamente su Ley n° 78-17, de 6 de enero de 1978 relativa à l'informatique, aux fichiers et aux libertés, a través de la Ley n° 2018-493, de 20 de junio de 2018, al objeto de ejercer ese "margen de maniobra nacional" autorizado por el RGPD, de acercar ciertas disposiciones a la letra del mismo e implementar la Directiva 680/2016 a la legislación francesa. Así mismo, ha modificado su Decreto de aplicación para adaptarlo a la mencionada Ley (Decreto n° 2018-687, de 1 de agosto de 2018).

Austria, tempranamente, llevó a cabo una modificación de calado de su Ley de protección de datos de 2000, mediante Ley Federal - Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018), de 31 de julio de 2017, para adaptarse al RGPD. Conviene observar que el § 70.(1) de la Datenschutzgesetz-DSG (2018), relativo a la entrada en vigor, excluía la aplicación hasta el 25 de mayo de 2018 de distintas secciones de títulos y

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

artículos, así como algunas de las rúbricas. A *sensu* contrario, enumeró los artículos, capítulos y parte de los mismos que dejaban de estar vigentes tras el 24 de mayo en la Ley de protección de datos de 2000.

Italia también aprobó el Decreto Legislativo nº. 101, de 10 de agosto de 2018, para la adecuación de la normativa nacional «alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)» (*G.U.*, n. 205, 4-9-2018).

Otros países, por ejemplo, Alemania, Reino Unido, Irlanda o España han optado por una nueva ley de protección de datos. Alemania aprobó tempranamente su nueva Ley Federal de Protección de Datos, de 30 de junio de 2017 (Bundesdatenschutzgesetz, BGBI. I S.2097). La ley federal alemana adapta el RGPD e implementa la Directiva 2016/680. Reino Unido, por su parte, aprobó la Data Protection Act el 23 de mayo de 2018, y también ha implementado la Directiva 2016/280. Llama la atención la parte cuarta de la ley referida al "Intelligence Services Processing" y los seis capítulos que la integran (arts. 82 a 113). Irlanda aprobó su Data Protection Act de 2018 y en la parte sexta del mismo se incluyen los artículos referidos al "Enforcement of data protection regulation and Directive" (arts. 105 a 156).

España llega con cierto retraso a la aprobación de su nueva ley de protección de datos que, sin embargo, está a punto de ser aprobada y publicada en el BOE. De hecho, el Gobierno debió aprobar el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa europea en materia de

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

protección de datos[2]. El contenido de este real decreto ley solo ha afectado a cuestiones cuya inmediata incorporación al Derecho interno resultaban imprescindibles para la adecuada aplicación del RGPD hasta la entrada en vigor de la nueva ley. Efectivamente, como expresamente prevé la disposición final única del real decreto ley, la vigencia del mismo se limita al período que media entre el día siguiente de su publicación en el Boletín Oficial del Estado hasta la vigencia de la nueva ley orgánica de protección de datos.

No obstante, y por lo que afecta al ordenamiento español, lo que se ha tramitado como proyecto de ley orgánica de protección de datos de carácter personal[3] en su tramitación parlamentaria se ha convertido, finalmente, en la Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales (LOPDGD).

Según dispone el art. 1 de la LOPDGD, "La presente ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

[2] Convalidado por el Congreso de los Diputados el 6 de septiembre de 2018 (*BOE*, n. 224, de 15 de septiembre de 2018).

[3] El Gobierno presentó el proyecto de ley orgánica de protección de datos de carácter personal el 14 de noviembre de 2017 (*BOCG*, Congreso de los Diputados, serie A, n. 13-1, de 24 de noviembre de 2017).

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

Editoriale

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el art. 18.4 de la Constitución".

En la fase de presentación de enmiendas en el Congreso de los Diputados[4], y tras la fase de discusión y aprobación de las mismas, se incorporó un nuevo título X rubricado "Garantía de los derechos digitales" (arts. 79 a 97). Y si bien es cierto que algunos de los derechos allí contenidos se prevén en el RGPD, no es menos cierto que otros derechos se reconocen de forma expresa. Entre otros, destacan el derecho de acceso universal a Internet (art. 81), el derecho a la seguridad digital (art. 82), el derecho a la educación digital (art. 83) o el derecho a la desconexión digital en el ámbito laboral (art.88).

Obsérvese que en la exposición de motivos de la LOPDGD expresamente se hace alusión a la necesidad de que, y cito textualmente, "una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales". Sin embargo, y en tanto no se acometa este reto, el legislador aborda el reconocimiento de un sistema de garantía de los derechos digitales a través de la inclusión de un nuevo título, el X, que

[4] *BOCG*, Congreso de los Diputados, serie A, n. 13-2, de 18 de abril de 2018, pp. 1-254.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

inicialmente no estaba previsto en el proyecto de ley de protección de datos que el Gobierno presentó al Congreso de los Diputados.

Sin duda, los retos de homogeneización normativa que plantea el RGPD a efectos de garantizar el derecho fundamental al tratamiento de los datos personales en la UE distan de ser sencillos. A día de hoy, solo basta con acudir a los acuerdos alcanzado en la tercera sesión plenaria del nuevo Comité Europeo de Protección de Datos celebrada los días 25 y 26 de septiembre de 2018. En esta sesión se llegó, entre otros, a un acuerdo que establece criterios comunes para las listas de evaluación de impacto en la protección de datos (DPIA)[5] y que constituyen una herramienta de enorme calado a los efectos de que en toda la UE el RGPD se aplique de forma coherente –arts. 35.4 y 35.6 RGPD-. De hecho, también se adoptó un nuevo proyecto de guía sobre el ámbito territorial que ayudaría a proporcionar una interpretación común sobre el alcance territorial del RGPD.

Pero no solo, la complejidad de los retos a los que se enfrenta la norma europea y su homogeneización en la UE se anuda al imparable progreso tecnológico que no puede ser aprehendido por una norma europea que nunca estará al alcance de garantizar un derecho con la misma eficacia y prontitud que le puede exigir el inexorable avance

[5] Se basa sobre las posiciones mantenidas por 22 Estados miembros (Austria, Bélgica, Bulgaria, República Checa, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Malta, Holanda, Polonia, Portugal, Rumania, Eslovaquia, Suecia y Reino Unido). Llama la atención que España no aportara nada sobre el particular, salvo error, en la página del Comité europeo (https://edpb.europa.eu/our-work-tools/our-documents_en).

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VIII, n. 2, 2018
data di pubblicazione: 12 marzo 2019

tecnológico. Sin embargo, el RGPD prevé mecanismos para tratar de superar esa obsolescencia jurídica y abordar algunos de los retos que la tecnología irremediablemente le va a deparar. En esta línea, no está de más recordar que, como establece el art. 97 del RGPD, a más tardar el 25 de mayo de 2020, y posteriormente cada cuatro años, la Comisión tendrá presentar al Parlamento Europeo y al Consejo una evaluación y revisión del reglamento y, en caso necesario, "las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información" (art. 97 del RGPD).

Solo me resta añadir, como ya he puesto de relieve en otro lugar, que si los retos que plantea el nuevo marco europeo de protección de datos revisten complejidad, no es menor el cambio de paradigma que se está imponiendo en la dogmática de los derechos fundamentales al permear y afectar el derecho a la protección de los datos personales, si bien con distinta intensidad, en el ejercicio de la mayoría de los derechos constitucionales en los diversos ordenamientos nacionales, con sus propias peculiaridades, sus distintas tradiciones jurídicas y sus más o menos acertadas técnicas de sistematización legislativa.