Nuevo Reglamento Europeo de Protección de Datos

Un enfoque global en la protección de Datos Personales en la Unión Europea

ARACELI CASAMAYOR DE BLAS
Universitat Jaime I

Resumen

El nuevo Reglamento Europeo de Protección de Datos es ya una realidad inminente. Según lo previsto, entrará en vigor en mayo de 2018 y, como cualquier otro reglamento comunitario, tendrá eficacia directa en todos los Estados Miembros de la Unión Europea.

Se aborda aquí una visión global del nuevo marco legislativo partiendo de la configuración constitucional de este derecho a la protección de datos y de su desarrollo comunitario.

Palabras clave: Protección de Datos, Unión Europea, Globalización, Derechos Fundamentales, TIC, Big Data.

Abstract

Complying with new requirements for the protection of personal data, in an increasingly globalised European framework and digital, the new Regulation European Data Protection is now an imminent reality. As expected, it will enter into force in may 2018 and, as any Community regulation, will have direct efficiency in all the Member States of the European Union.

An overview of the new legislation on the basis of its Fundamental Right definition is dealt with here and the legal challenges it is facing.

Key words: Data Protection, European Union, Globalised world, Fundamental Rights, TIC, Big Data.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

Abreviaturas

LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
RGPD UE	Reglamento 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.
DPO	Data Protecttion Officer.
TFUE	Tratado de Funcionamiento de la Unión Europea.
UE	Unión Europea.
AGPD	Agencia Española de Protección de Datos.

1. Introducción

En abril de 2016, fue aprobado por el Parlamento Europeo el nuevo Reglamento General de Protección de Datos, por el que quedará derogada la Directiva 95/46/CE[230] y que será de aplicación directa en todos los países miembros de la Unión Europea, sin necesidad de transposición legal y en el plazo de dos años a contar desde su entrada en vigor, esto es, el 25 de mayo de 2018.

En un marco europeo cada vez más globalizado, bajo el que la tecnología ha transformado el ámbito empresarial y los datos personales han adquirido una enorme relevancia, en particular, en el área del Big Data, permitiendo que, tanto las entidades públicas como las empresas privadas estén utilizando datos personales a una escala sin precedentes a la hora de realizar sus actividades. De igual manera, en el ámbito más privado del día a día de los ciudadanos, las personas difunden un volumen cada vez mayor de información personal a un nivel mundial.

Podría decirse que los datos personales son el petróleo del Siglo XXI y, por ello, conseguir una sólida protección para los mismos sea probablemente una de las cuestiones jurídicas más complejas, a la vez que ineludible, a las que se enfrenta el Estado Moderno.

Con el RGPD UE se dibuja un marco legal más exigente que el previsto en la vigente Directiva 95/46 y, más próximo al establecido en España desde hace más de diecisiete años con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).

Este nuevo Reglamento unifica en gran medida el marco legal que actualmente se aplica en este ámbito, añade derechos y obligaciones y modifica la forma de dar cumplimiento a algunos de ellos ya existentes. Además, aborda cuestiones tan novedosas como la creación

230 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.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

de perfiles o la seudonimización, el procesamiento de *Cloud Computing* (la popular nube informática) y *Big Data*, e incorpora los principios del análisis de riesgos y la privacidad por diseño y por defecto.

No cabe duda de que nos encontramos ante la reforma de mayor relevancia que se ha adoptado en los últimos años en el ámbito de la protección de datos y la privacidad, cuyo principal objetivo es la aplicación uniforme y coherente del derecho de protección de datos en el territorio de la Unión Europea. A su vez, el nuevo Reglamento pretende cambiar la manera de ver y entender el derecho a la privacidad, pasando a un enfoque preventivo. A partir de ahora, las organizaciones pasan a ser responsables de analizar sus riesgos y diseñar medidas apropiadas a los mismos.

En este sentido, el marco global de la privacidad queda también delimitado por los principios de toda sociedad democrática y respetuosa con los Derechos Fundamentales, como son la libertad de expresión, la transparencia y el acceso a la información.

Es importante destacar que, conforme a su artículo 3**,** la nueva norma afectará a organizaciones, entidades y empresas que, aunque no estén establecidas en territorio europeo, ofrezcan bienes y servicios en la Unión Europea o monitoricen sus conductas de comportamiento. Lo que implica directamente que, el nuevo RGPD, se aplicará también al tratamiento de datos fuera de la Unión Europea, ampliando significativamente su ámbito de aplicación.

2. Marco jurídico del derecho a la protección de datos

La protección de datos personales es un Derecho Fundamental recogido en el artículo 18.4 de la Constitución española - así como en la inmensa mayoría de las Constituciones europeas - sobre el derecho a la intimidad familiar y personal y el secreto de las comunicaciones, estableciendo que *la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*, límite que se traduce en la potestad de control sobre el uso que se hace de los datos personales.

Este control permite evitar que, a través del tratamiento de nuestros datos, se pueda llegar a disponer de información sobre nosotros que afecte a nuestra intimidad y demás Derechos Fundamentales y Libertades Públicas.

La Sentencia del Tribunal Constitucional 45/1999, de 22 de marzo[231] señaló ya que nos encontramos ante un Derecho Fundamental a la protección de datos por el que se garantiza

[231] Sentencia 45/1999, de 22 de marzo de 1999 del Tribunal Constitucional. Recurso de Amparo núm.2460/1996

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

a la persona el control, uso y destino sobre los mismos. De esta forma, el derecho a la protección de datos se configuraba como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos de los que justificaron su obtención. Sin embargo, con esta primera pronunciación del Alto Tribunal y las que la siguieron, se reconocía el derecho a la protección de datos personales de una manera ciertamente confusa y, no fue hasta mucho más tarde, con la *STC 292/2000, de 30 de noviembre*[232], cuando en una mejor perfilación del mismo, el Tribunal Constitucional consideró este derecho a la protección de datos como un derecho autónomo e independiente. Consistiendo el mismo en un poder de disposición y de control sobre los datos personales y facultando a los usuarios de decidir cuáles de esos datos proporcionar a un tercero, sea el Estado, o un particular y dotándolo de plena autonomía respecto del derecho a la intimidad.

En el ámbito europeo, el Derecho a la protección de datos está reconocido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01) como sigue:

> 1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
>
> 2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
>
> *3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.*

De igual manera, en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (antiguo art. 286 TCE), se reconoce que *cada persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

Con la nueva reforma comunitaria dichos artículos se encuentran desarrollados en el RGPD UE, garantizando de este modo un nivel de protección equivalente en todos los Estados miembros.

Actualmente, con la LOPD, España tiene una de las legislaciones más avanzadas de la Unión Europea en materia de protección de datos, es importante recordar que, la Directiva relativa a la protección de datos de 1995 significó un verdadero avance en la protección de los datos personales en la Unión Europea, consagrando dos de las más antiguas ambiciones del proceso de integración comunitaria, por un lado, la protección de los Derechos y libertades fundamentales de las personas, en particular, del Derecho Fundamental a la protección de

[232] Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

datos, y, por otro, la realización del mercado interior, en este caso, la libre circulación de datos personales.

Con la entrada en vigor de este nuevo RGPD, en España, la LOPD seguirá siendo plenamente válida y aplicable en lo que esté fuera del Derecho de la UE, el propio Reglamento hace, además, numerosas remisiones a la legislación nacional de los Estados miembros.

3. Concepto de dato de carácter personal y otros términos asimilados

Antes de profundizar en el nuevo Reglamento Europeo de Protección de Datos convendría dilucidar qué es un dato de carácter personal y, sobretodo, en qué consiste este Derecho a la protección de datos personales.

El concepto dato de carácter personal se define legalmente en el artículo 3. a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el artículo 5.1 f) de su Reglamento como sigue: *cualquier información numérica, alfabética, gráfica, acústica, fotográfica o de cualquier otro tipo que permita identificar a una persona o hacerla identificable.*

El elemento fundamental para determinar qué se trata de un dato de carácter personal es que la información, por sí misma o combinada, como puede ser un nombre, apellidos, estado civil, correo electrónico, etc. permita saber a quién pertenece ese dato o que pudiese averiguarse con facilidad. Bien por estar directamente identificada a través de algún dato, o bien porque pueda llegar a ser identificada por otro medio. Por consiguiente, no es necesario que la persona se encuentre totalmente identificada, sino que basta que resulte identificable.

A su vez, existe una diferenciación entre los diferentes datos de carácter personal, que la Agencia Española de Protección de Datos establece de la siguiente manera:

a) Datos especialmente protegidos: vida sexual, ideología, salud, etc.

b) Datos de carácter identificativo: DNI/NIF, firma, huella, dirección, etc.

c) Datos relativos a las características personales: fecha de nacimiento, sexo, nacionalidad, etc.

d) Datos relativos a las circunstancias sociales: propiedades, aficiones, etc.

e) Datos académicos y profesionales.

f) Datos que aportan información comercial: actividades y negocios, creaciones artísticas, científicas etc.

g) Datos económicos, financieros y de seguros.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

h) Datos relativos a transacciones de bienes y servicios: transacciones financieras, indemnizaciones, etc.

Sentadas estas bases, resultará más sencillo el acercamiento desde un punto de vista técnico al tema que nos aborda.

4. Principales aspectos del nuevo marco normativo

4.1. Nuevos derechos

Con el fin de otorgar una mayor y más efectiva protección a los datos de los ciudadanos en la Unión Europea, el Reglamento incorpora nuevos derechos, tales como el derecho a la limitación del tratamiento o el derecho a la portabilidad de los datos y consolida tradicionales derechos ya regulados anteriormente de manera expresa como son el derecho al olvido, de acceso, rectificación, cancelación y oposición adaptándolos a la más reciente jurisprudencia europea en este ámbito.

4.1.1. Derecho a la portabilidad de datos de un prestador de servicios a otro

Reconocido en el artículo 20 RGPD UE, el derecho a la portabilidad establece que el interesado tendrá derecho a recibir cualesquiera dato personal que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado cuando sea técnicamente posible. Nos referimos aquí a datos tratados mediante medios automatizados.

Únicamente podrán ser portados aquellos que hubieran sido facilitados por el interesado, lo que excluye, en principio, los generados por el propio responsable. Así como tampoco podrá aplicarse tal derecho cuando el tratamiento sea necesario para el cumplimiento de un proceso realizado en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Este nuevo derecho aportará para los interesados transparencia y un mayor control sobre sus datos.

4.1.2. Derecho a la limitación del tratamiento

Reconocido en el artículo 18 del RGPD UE, el derecho a la limitación del tratamiento implica que el responsable del tratamiento podrá conservar los datos pero no podrá tratarlos sin el consentimiento del afectado o cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, la protección de los derechos de otra persona física o jurídica, o por razones de interés público.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

4.1.3. Derecho al olvido o derecho de supresión

En este caso, no se trata de un nuevo derecho introducido por el RGPD UE, sino de una adaptación del mismo a la jurisprudencia europea más reciente en la materia. Como se sabe, en mayo de 2014, el Tribunal de Justicia de la Unión Europea con el conocido *Caso Google*[233] respondiendo a una cuestión prejudicial de interpretación planteada por la Audiencia Nacional, abordó, por primera vez, el tema bajo el prisma de los medios de comunicación, las hemerotecas y ese difícil equilibrio entre dos Derechos Fundamentales: el derecho a la privacidad frente a la libertad de información en relación con la información suministrada por los motores de búsqueda en internet, en concreto con la empresa Google. Fallo en el que, por primera vez, se reconocía el derecho a solicitar, bajo ciertas condiciones, la retirada de datos por parte del buscador.

Este denominado derecho al olvido es la manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores de internet. Con este derecho se reconoce al ciudadano la legitimación para impedir la difusión de información personal a través de internet, cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original fuere legítima, como puede ser en el caso de boletines oficiales o informaciones amparadas por las libertades de información o de expresión.

La legislación española establece que para ejercer los derechos de cancelación y oposición y, por tanto, el derecho al olvido es imprescindible que el ciudadano se dirija en primer lugar a la entidad que está tratando sus datos, en este caso al buscador. Los buscadores mayoritarios, Google, Yahoo y Bing, han habilitado ya sus propios formularios para recibir las peticiones de ejercicio de estos derechos. Si la entidad no diese respuesta a la petición realizada o el ciudadano considera que la respuesta que recibida no es la adecuada, podría solicitar que la Agencia Española de Protección de Datos tutele su derecho frente al responsable. En función de las circunstancias de cada caso concreto, la Agencia determinará si lo estima o no. Siendo esta decisión de la Agencia, a su vez, recurrible ante los Tribunales.

4.1.4. Derecho de información en la recogida de datos

Este derecho se concreta en el derecho a obtener una información transparente, leal, lícita y de fácil acceso a los interesados sobre el tratamiento de sus datos, reconocido en el Artículo 5 RGPD UE. Estableciendo a su vez, que en el tratamiento y recogida de datos de carácter personal, será necesario informar previamente a los interesados, a través del medio que se utilice para la recogida, de modo expreso, preciso e inequívoco:

[233] *Sentencia 13-5-14, asunto C-131/12, Google Spain, S.L., Google Inc. vs Agencia Española de Protección de Datos (AEPD), Mario Costeja González -EDJ 2014/67782-.*

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

1) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

2) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

3) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

4) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

5) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Con el nuevo Reglamento se actualizan los conocidos en España como derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), estableciéndose que, se deberá adecuar el procedimiento de gestión y atención de estos derechos al RGPD UE como sigue:

4.1.5. Derecho de cancelación

Este derecho de cancelación se reconoce con el fin de que los propios ciudadanos puedan controlar por sí mismos el uso que se hace de sus datos personales y, en particular, el derecho a que éstos se supriman cuando resulten inadecuados o excesivos, sin perjuicio del deber de bloqueo recogido en la LOPD.

De igual manera que el resto de Derechos ARCO, su ejercicio es personalísimo, por lo que sólo podrá solicitarlo la persona interesada, quien deberá dirigirse a la empresa u organismo público que sabe o presume que tiene sus datos, indicando a qué datos se refiere y, aportando al efecto la documentación que lo justifique.

4.1.6. Derecho de oposición

El derecho de oposición es uno de los derechos que la LOPD reconoce a los ciudadanos para que puedan defender su privacidad controlando por sí mismos el uso que se hace de sus datos personales, y en particular, el derecho a que no se lleve a cabo el tratamiento de éstos o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario.

4.1.7. Derecho de acceso

Este derecho de acceso de los afectados a sus propios datos personales se encuentra reconocido en el artículo 15 RGPD como sigue *el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.*

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

Con este derecho de acceso, se pretende, ni más ni menos, lograr un Derecho de acceso más fácil a los datos personales.

4.1.8. Derecho de rectificación

Este derecho se caracteriza porque permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

Como el resto de derechos ARCO, su ejercicio es personalísimo, por lo que sólo podrá solicitarlo la persona interesada, quien deberá dirigirse a la empresa u organismo público que sabe o presume que tiene sus datos, indicando a qué datos se refiere, la corrección que se solicita y, aportando al efecto la documentación que así lo justifique.

4.2. Un nuevo Reglamento, dos nuevas figuras para la Protección de Datos

Entre las medidas que contempla la nueva normativa comunitaria, respecto del régimen actual, destaca la exigencia de que toda empresa que trate datos personales deberá adaptarse, con el fin de garantizar el cumplimiento de la normativa y en los supuestos establecidos, a una serie de nuevas obligaciones concretadas en dos nuevas figuras, la figura del Delegado de Protección de Datos y una Autoridad de control.

El fundamento de estas nuevas figuras se encuentra en lo que se conoce como responsabilidad activa, que no es otra cosa que la prevención por parte de las organizaciones que tratan datos, estas nuevas exigencias reflejan el carácter preventivo que pretende instaurar el nuevo reglamento. Las empresas deberán adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el nuevo RGPD establece.

4.2.1. Data Protection Officer

La figura del *Data Protection Officer,* o lo que es lo mismo, un Delegado de Protección de Datos, ha sido objeto de intensos debates sobre su carácter obligatorio o no para todas las entidades e instituciones. Finalmente, el nuevo Reglamento establece que este DPO será un instrumento voluntario, excepto en organizaciones e instituciones públicas y en empresas con más de 250 trabajadores.

En el caso de entidades con menos de 250 empleados, será obligatorio cuando se de alguna de las siguientes circunstancias:

> **1)** Que el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
>
> **2)** Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

3) Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

4) El tratamiento de datos relativos a condenas e infracciones penales.

En cuanto a sus funciones, pese a que las entidades podrán determinar y ampliar sus funciones, las mínimas establecidas son las que siguen:

1) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

2) Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes.

3) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación así como cooperar con la autoridad de control.

4) Actuar como punto de contacto de *la Autoridad de Control* para cuestiones relativas al tratamiento, incluida la consulta previa y realizar consultas, en su caso, sobre cualquier otro asunto.

4.2.2. Autoridad de Control

La Autoridad de control será el organismo que en cada Estado Miembro regule, supervise y vigile el tratamiento de datos de carácter personal.

El responsable, el encargado del tratamiento y, en su caso, sus representantes cooperarán con la Autoridad de Control que lo solicite en el desempeño de sus funciones y ante este organismo se deberán realizar entre, otras cosas:

1) Consultas previas tras evaluaciones de impacto de alto riesgo.

2) Notificaciones de violaciones de seguridad de datos.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

Para las entidades establecidas en varios Estados miembros o que, estando en un solo Estado miembro, realice tratamientos que pudiesen afectar a ciudadanos en varios Estados de la Unión Europea se introduce el concepto de *ventanilla única*, que se traduce en que los empresarios tendrán una única Autoridad de protección de datos como único supervisor en Europa, lo que, por otro lado, se estima representará un considerable ahorro económico para la UE.

A su vez implica también que, a partir de la entrada en vigor del Reglamento, cada Autoridad de protección de datos europea, en lugar de analizar una denuncia o autorizar un tratamiento a nivel nacional, valorará si el supuesto tiene carácter transfronterizo y en cuyo caso dará lugar a un procedimiento de cooperación entre todas las Autoridades afectadas, con el fin de buscar un solución beneficiosa para todas ellas. En caso de discrepancias, el caso será elevado al Comité Europeo de Protección de Datos, un organismo de la Unión integrado por los directores de todas las Autoridades de protección de datos de la UE. Este Comité resolverá la controversia mediante decisiones vinculantes para las Autoridades implicadas.

Por otro lado, este nuevo sistema no supone que los ciudadanos tengan que relacionarse con varias Autoridades o con Autoridades diferentes de la del Estado donde se resida, sino que, de igual manera, la reclamación se planteará ante la propia Autoridad nacional - para los españoles, la Agencia Española de Protección de Datos - que será, también, la responsable de informar al interesado del resultado final de su reclamación o denuncia.

Para las entidades establecidas en varios Estados miembros, la Autoridad de control principal que resultará competente será la del lugar donde el responsable cuente con su establecimiento principal. En caso de grupos de empresa radicadas en la Unión Europea, será la que se corresponda con su sede central de operaciones.

Entre otros supuestos, bajo este nuevo marco legal, la autorización de la Agencia Española de Protección de Datos dejará de ser necesaria para transferir datos a terceros países cuando se usen las cláusulas contractuales tipo adoptadas por la Comisión Europea, una Autoridad de control o normas corporativas vinculantes.

Asimismo, se encuentra prevista la creación de un Consejo Europeo de Protección de Datos, este Consejo, según lo previsto, estará formado por los representantes de cada una de las Autoridades de control independiente y será el encargado de velar por los derechos de los usuarios en esta materia y de preservar la debida protección de sus datos personales.

4.3. Nuevas obligaciones

Con la entrada en vigor del nuevo RGPD UE, se establece un nuevo sistema de recogida de datos, concretado en nuevas formas de información al interesado mediante un sistema armonizado para todos los países de la Unión Europea. Así pues, las cláusulas informativas y políticas de privacidad deberán adaptarse a un nuevo conjunto de deberes informativos para las entidades que traten datos personales, como son, la creación de un Registro de las

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

actividades de tratamiento, nuevos plazos de conservación de los datos, el derecho a presentar reclamación ante la autoridad de control competente, todo ello en virtud del principio de transparencia.

4.3.1. Registro de las actividades de tratamiento

La creación de un Registro de las actividades de tratamiento será obligatorio para toda empresa que trate datos de carácter personal, tal y como establece el artículo 30 del RGPD; este Registro sistematizará las actividades vinculadas al tratamiento de datos y estará a disposición de las autoridades competentes en caso de que lo soliciten.

A estos efectos, por aplicación del art. 4.2 RGPDUE, se entiende por tratamiento *cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.*

4.3.2. Evaluaciones de impacto (*Privacy Impact Assessments*, PIA)

Esta evaluación de impacto introducida con el artículo 33 del RGPD UE tiene como objetivo minimizar los riesgos que un tratamiento de datos puede plantear para los ciudadanos, será, por tanto, obligatoria cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas. Y una única evaluación servirá para abordar operaciones de tratamiento similares que planteen riesgos elevados similares.

El responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, esta evaluación de impacto podrá ser recomendada, propuesta, dirigida y coordinada por el DPO en aquellos casos en que sea necesario, esto se dará, sí o sí, cuando las empresas traten alguno de los siguientes aspectos:

1) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

2) Tratamiento a gran escala de las categorías especiales de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

3) Tratamiento de datos personales relativos a condenas e infracciones penales.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

4) Observación sistemática a gran escala de una zona de acceso público.

4.4. Un nuevo régimen sancionador

Bajo este marco, en caso de vulneración de los derechos reconocidos por este RGPD, los interesados y en determinadas condiciones, también las organizaciones de protección de datos, podrán presentar reclamaciones ante una Autoridad de control o interponer recurso en caso de que no se cumplan las normas de protección de datos.

En el supuesto de infracción de la normativa establecida o por incumplimiento de las resoluciones de la autoridad de control, el nuevo Reglamento dispone que los responsables del tratamiento pueden enfrentarse a multas de hasta 20.000.000 de euros y, para la empresas, el 4 % de su facturación anual, lo que supone una significativa elevación de la cuantía de las sanciones. Pudiendo establecerse, a su vez, la prohibición del tratamiento de datos en las empresas que incumplan las nueva normativa comunitaria y la suspensión de las transferencias internacionales de datos.

De igual modo, las empresas, que tienen obligación de comunicar en un plazo de 72 horas los riesgos de seguridad que pudieran sufrir, esto es, los "frecuentes" *ataques informáticos*, de no hacerlo, podrán ser objeto de las *class actions*. Definidas desde los parámetros conceptuales del derecho procesal como demandas colectivas por parte de los usuarios afectados, que podrán ejercitar acciones de defensa, no sólo de sus propios derechos e intereses, sino, además y de forma simultánea, en defensa de los análogos derechos e intereses de un número indeterminado de usuarios no identificados (*class members*).

4.4.1. Derechos Fundamentales, globalización y protección de datos

Como cualquier Derecho Fundamental, el derecho a la protección de datos personales no es un derecho absoluto, incondicionado o carente de limitaciones, sino que debe considerarse en relación con su función en la sociedad actual y, con arreglo al principio de proporcionalidad mantener el equilibrio con otros Derechos Fundamentales. Por consiguiente, podrá y deberá, en determinadas ocasiones, ceder ante otros valores y bienes constitucionales.

Que los Derechos Fundamentales tienen límites para garantizar otros Derechos y bienes constitucionales es doctrina reiterada de nuestro Tribunal Constitucional, sin embargo y en todo caso, los límites que se le impongan para garantizar otros derechos y valores constitucionales habrán de respetar su contenido esencial. En este sentido, se pronunció el Tribunal Constitucional con ocasión de la *STC 17/2013, de 31 de enero*[234], en la que, reiterando

[234] Sentencia 17/2013, de 31 de enero de 2013 sobre Administración y protección de datos.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

la fundamentación establecida en la *STC 292/2000, de 30 de noviembre*[235], estableció que si la Ley es la única habilitada por la CE para fijar los límites a los Derechos Fundamentales y, en el caso presente, al derecho a la protección de datos, esos límites no podrán ser distintos a los constitucionalmente previstos que, para el caso, no son otros que los derivados de la coexistencia de este Derecho Fundamental con otros derechos y bienes jurídicos de rango constitucional.

La gran mayoría de limitaciones de los Derechos Fundamentales nacen de su colisión con otros Derechos o principios igualmente fundamentales y, puesto que por su carácter de normas-principio no es posible establecer una jerarquía entre ellos, el equilibrio ha de alcanzarse mediante la ponderación de los intereses en conflicto en cada caso concreto. En consecuencia, cuando el Derecho a la protección de datos personales entre en conflicto con un principio o Derecho Fundamental será necesario realizar esta identificación de los intereses en conflicto en el caso concreto y efectuar su posterior juicio de razonabilidad.

Es bajo este marco que, la tensión entre libertad y seguridad a la hora de regular el Derecho a la protección de los datos personales constituye uno de los mayores desafíos a los que se enfrenta el Estado Moderno de nuestros días. El auge de nuevos medios de comunicación, una tecnología cada vez más sofisticada y la cada vez mayor implantación de soluciones de cruzamiento masivo de datos o *Big Data* y los nuevos modelos de mercado, venían exigiendo una legislación de mayor rigor y homóloga para todos los Estados miembros. El desarrollo de la normativa sobre protección de datos ha tenido, en realidad, desde sus inicios una tendencia a globalizarse.

Dentro de este proceso de globalización, las TIC, término que proviene de *tecnologías de la información y comunicación,* han sido determinantes en el propósito de lograr una mayor protección de nuestros datos. Integradas en la mayor parte de sectores, desde las Administraciones Públicas hasta entidades privadas o cualquier hogar. Cuando se habla de redes TIC nos referimos, en síntesis, a la telefonía móvil, las redes de internet, sistemas operativos de ordenadores, la banca online, el correo electrónico, etc.

Es bajo este panorama que la necesidad de una coexistencia de valores y principios en los que debe basarse un marco jurídico europeo, si no quiere renunciar a sus funciones de unidad e integración y al mismo tiempo ser compatible con una regulación firme, homogénea y completa, que proteja los derechos de los ciudadanos en una materia tan delicada como son los datos personales no era tarea fácil. La eterna dualidad entre lo positivo de este nuevo marco global digitalizado y el pretendido desiderátum de una real protección de nuestros datos personales. Al igual que Parménides dividió todas las cosas en positivas y negativas a excepción de una dualidad, nos preguntaríamos aquí, qué es lo positivo y qué es lo negativo

[235] Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

en este nuevo marco digital. Parece ser que, la levedad que nos aporta la tecnología conlleva el peso que supone la pérdida de control de nuestros datos personales. En este contexto, el Derecho Fundamental a la protección de datos debe constituir el punto de equilibrio necesario que garantice nuestra privacidad y control sobre estos datos.

5. Conclusiones

El nuevo Reglamento Europeo de Protección de Datos constituye uno de los mayores logros legislativos europeos de los últimos tiempos. Representa el inicio de una nueva etapa en el derecho de privacidad y la protección de datos con efectos a nivel global. Se caracteriza por un enfoque más garantista de los derechos de los ciudadanos, otorgando a los usuarios la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos. A su vez, ofrece mejores instrumentos para prevenir posibles infracciones.

En mi opinión, la previsión de un sistema basado en la responsabilidad activa o de prevención, constituye una de las novedades que puede resultar más favorable en la protección de los datos personales. Cuando se trata de un ámbito tan delicado, directamente relacionado con la protección a un Derecho Fundamental, como es la protección de datos personales, actuar sólo tras la infracción resultaba insuficiente.

Parece que en Europa han decidido tomarse la privacidad de nuestros datos personales muy en serio y, a partir del 25 de mayo de 2018, deberán hacerlo también las empresas que gestionen datos personales y sus administradores, que son los responsables últimos, si no quieren ser condenados por el nuevo y elevado régimen sancionador.

Con todo, debemos asentar la idea de que el desarrollo de las nuevas tecnologías va a ser permanente. No hay un punto de llegada. Por ello, este imparable progreso de digitalización que ahora venía exigiendo una legislación de mayor rigor en materia de protección de datos, requerirá, a su vez, una continua e incesante adaptación. La tarea no será fácil, pero sí necesaria.

6. Bibliografía

6.1. Legislación

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.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017

Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea (2012/C 326/01)

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. (1995).

Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea

2012/C 326/01.

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), de 4 de noviembre de 1950.

Fecha de recepción: 5/3/2017 Fecha de aceptación: 26/3/2017