diariolaley Wolters Kluwer

Se acerca el 25 de mayo de 2018. ¿Está su empresa adaptada al nuevo Reglamento de Protección de Datos?

Natalia MARTOS

Counsel de Pérez-Llorca

Área de Privacidad, IP/IT y Negocios Digitales

Diario La Ley, Nº 9081, Sección Tribuna, 15 de Noviembre de 2017, Editorial **Wolters Kluwer**

Normativa comentada

Regl. 2016/679 UE, de 27 Abr. (protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE -Reglamento general de protección de datos-)

Comentarios

Resumen

El Reglamento 2016/679 del Parlamento y del Consejo Europeo de 26 de abril de 2016, será de obligatorio cumplimiento a partir del **próximo 25 de mayo de 2018**. Adicionalmente, está en fase de tramitación parlamentaria el **Anteproyecto de Ley Orgánica de Protección de Datos.** Asimismo, comentaré los detalles relativos a la nueva figura del Delegado de Protección de Datos, tanto desde la perspectiva del Reglamento General de Protección de Datos como del Anteproyecto de Ley Orgánica de Protección de Datos.

En este artículo analizaremos las instituciones jurídicas derivadas de la nueva norma e incluiremos unas conclusiones.

I. *Antecedentes: la aplicación del Reglamento General de Protección de Datos europeo (en adelante, RGPD) y la próxima aprobación del Anteproyecto de Ley de Protección de Datos de Carácter nacional (en adelante, el Anteproyecto)*

El pasado 27 de abril de 2016 se aprobó el RGPD (LA LEY 6637/2016)con el objetivo de proteger los datos personales de los individuos que, conforme al art. 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea (LA LEY 12415/2007) y al 16.1 de Tratado de Funcionamiento de

la Unión Europea, (LA LEY 6/1957) es un **derecho fundamental.** El RGPD establece que «el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales» como, por ejemplo, la libertad de empresa. La rápida evolución tecnológica y la globalización han planteado nuevos retos a la protección de este derecho fundamental. La tecnología ha transformado tanto la economía como la vida social y ha de facilitar la libre circulación de datos tanto dentro de la Unión como entre terceros países, garantizando un elevado nivel de protección de los datos personales.

En los Considerandos del RGPD, se nos informa de que «estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea» pero que no impida que la economía digital se desarrolle en el mercado interior.

No será hasta el 25 de mayo de 2018 cuando sea plenamente exigible el cumplimiento del RGPD

Si bien el RGPD fue aprobado el 27 de abril de 2016 y entró en vigor 20 días después de esa fecha, no será hasta el 25 de mayo de 2018 cuando sea plenamente exigible su cumplimiento. Con este plazo de dos años, se ha intentado promover la adaptación de empresas, administraciones y otros organismos a la nueva normativa que incluye nuevas figuras e instituciones jurídicas que cambian radicalmente el panorama normativo en materia de protección de datos.

Adicionalmente, el RGPD establece que «sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento». Asimismo, los Estados miembros están facultados para adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación del RGPD.

A estos efectos, a nivel nacional, está en tramitación parlamentaria el Anteproyecto que será analizado a continuación del RGPD en el presente documento. A pesar de que esta norma viene a completar la aplicación del RGPD, este último es de aplicación directa a todos los sujetos de los Estados miembros por lo que, si el Anteproyecto no estuviera formalmente aprobado por las Cortes el 25 de mayo de 2018, la única norma de aplicación sobre esta materia será el RGPD.

II. *Principales novedades introducidas RGPD*

1. *Ámbito de aplicación territorial*

Dentro del CAPÍTULO I, *Disposiciones Generales*, el art. 3.2 (LA LEY 6637/2016)introduce una importante novedad en relación con el régimen jurídico vigente, recogido en la Ley Orgánica 15/1999, de 13 de diciembre (LA LEY 4633/1999), de Protección de Datos de Carácter Personal, ampliando el ámbito territorial del RGPD a todo responsable o encargado no establecido en la Unión, cuando las actividades relacionadas con el tratamiento consista en la oferta de bienes o servicios a ciudadanos europeos o bien si controlan el comportamiento de los mismos, por ejemplo, haciendo perfilado de usuarios.

Entre los argumentos que señalan los considerandos del RGPD para justificar la ampliación del ámbito territorial está en la garantía de que los ciudadanos europeos no se vean privados de su derecho fundamental a la protección de datos por el mero hecho de que el encargado o responsable resida fuera de la Unión. Esta novedad *afecta de forma drástica a los gigantes tecnológicos norteamericanos* que, hasta la fecha, han venido nutriendo sus bases de datos, ya sean redes sociales, servicios de email gratuito y análogos con datos de ciudadanos de la Unión Europea con el consiguiente riesgo al no ser los Estados Unidos de América un país con un nivel de protección de datos equiparable a la Unión. En este sentido, a partir de 25 de mayo de 2018, estas y cualesquiera empresa radicada en cualquier parte del mundo que cumpla con los requisitos del art. 3 del RGPD (LA LEY 6637/2016)estará sujeta, como cualquier empresa europea a dicha norma.

2. *Deber de transparencia: obtención del consentimiento, deber de información y nuevos derechos de los ciudadanos*

La obtención del consentimiento se articula de una manera mucho más formal de lo que se venía haciéndose en la regulación vigente. Hasta la plena aplicación del RGPD son válidos los consentimientos obtenidos mediante la mera inacción del usuario, el uso de casillas pre-marcadas y demás subterfugios para evitar el conocimiento total por parte del titular del dato. Con el RGPD, se exige máxima transparencia y este requisito demanda que el responsable demuestre que obtuvo el consentimiento por parte del usuario de una manera libre, mediante una acción proactiva y concreta para cada una de las finalidades del tratamiento como marca su art. 7 (LA LEY 6637/2016).

A los efectos de conseguir esta transparencia en la obtención del consentimiento, se refuerzan los requisitos de información de una manera ostensible en relación con la vigente normativa. Como

novedad, el responsable, antes de obtener el consentimiento del titular del dato, deberá informar, entre otros: de los datos del delegado de protección de datos; de la intención de transferir sus datos a terceros estados; del plazo de retención de los datos; información sobre cómo ejercer los nuevos derechos que otorga el RGPD al interesado o el derecho a presentar una reclamación ante una autoridad de control.

Otra de las novedades que incluye el RGPD son nuevos derechos a favor del titular de dato como son:

- El **derecho a la portabilidad** de los datos: el interesado podrá solicitar al responsable todos los datos personales que le incumban en un formato estructurado e incluso podrá solicitar que transmita esos datos a otro responsable.
- El **derecho al olvido** y el derecho a **la limitación del tratamiento** que vienen a ofrecer garantías de protección adicionales derivadas del desarrollo de la tecnología.

3. *La responsabilidad proactiva*

El conocido como principio de *Accountability* ha sido traducido al español como «responsabilidad proactiva» y se constituye como uno de los pilares fundamentales del RGPD tal y como se describe claramente en su Considerando (74). (LA LEY 6637/2016) Se trata de que los responsables del tratamiento estarán obligados a aplicar las medidas oportunas y eficaces para mantener la integridad y el adecuado tratamiento. Pero, adicionalmente, la responsabilidad proactiva exige que el responsable pueda demostrar, en cualquier momento, que ha adoptado las medidas necesarias para ello frente a las autoridades competentes. Así, en su art. 5.1, (LA LEY 6637/2016) el RGPD señala que el responsable del tratamiento deberá tratar los datos de manera «responsable» y deberá ser capaz de demostrarlo.

A los efectos de dar cumplimiento con este mandato, se introducen las siguientes novedades:

- La adhesión a **códigos de conducta** aprobados conforme establece la norma o estar **certificado** según la misma podrán ser elementos suficientes para probar la responsabilidad del responsable del tratamiento (art. 24 (LA LEY 6637/2016)).
- La **protección de datos desde el diseño y por defecto** garantiza que el responsable del tratamiento aplicará las medidas técnicas y organizativas necesarias para asegurar que sólo serán objeto de tratamiento los datos personales que sean necesarios para cada finalidad (art. 25 (LA LEY 6637/2016)).

• El **registro de las actividades** de tratamiento. Las empresas responsables estarán obligadas a llevar un libro «diario» donde registren todos los tratamientos que efectúan; indicando el responsable y el delegado de protección de datos de un tratamiento determinado, los fines del tratamiento, una descripción de categorías de datos personales, entre otras obligaciones (art. 30 (LA LEY 6637/2016)).

• La **evaluación de impacto** se erige como una institución fundamental para el cumplimiento del RGPD. Si bien la nueva norma elimina el deber de registro de los ficheros ante la autoridad competente, exige como contrapartida que el responsable del tratamiento analice todos y cada uno de los tratamientos de datos que pudieran entrañar un riesgo para los derechos y libertades de las personas físicas. La evaluación de impacto será obligatoria en aquellos casos en los que se realice un perfilado de datos personales, o bien se traten categorías especiales de datos tales como los de salud, orientación sexual, raza o tendencias políticas, entre otros, así como cuando el responsable realiza una observación a gran escala de datos en una zona de acceso público. Como veremos a continuación, el Anteproyecto establece una lista de tratamientos que requieren realizar una previa evaluación del impacto. La evaluación de impacto deberá contener, como mínimo: descripción del tratamiento e interés legítimo perseguido por el mismo; evaluación de la necesidad y proporcionalidad del tratamiento; evaluación de los derechos y libertades de los sujetos afectados y las medidas previstas en caso de poner el riesgo dichos derechos y libertades (art. 35 (LA LEY 6637/2016)). En caso de que el resultado conlleve un posible riesgo para los sujetos afectados por el tratamiento, el responsable deberá hacer una consulta previa a la autoridad de protección de datos. Si la acción examinada no reporta un riesgo, podrá llevarse a cabo y el responsable conservará, en su registro de actividades, la evaluación de impacto realizada.

4. *La seguridad de los datos personales: la notificación de brechas de seguridad*

Aunque bien pudiera estar encuadrado en el apartado b) anterior por ser otra de las responsabilidades proactivas de las empresas responsables de tratamiento de datos personales, merece un análisis separado por su relevancia y novedad.

En caso de violación de seguridad de los datos personales, el responsable del tratamiento lo notificará a la autoridad de control en un plazo máximo de 72 horas

Conforme al art. 33 (LA LEY 6637/2016), en caso de violación de seguridad de los datos personales, el responsable del tratamiento lo notificará a la autoridad de control no más tarde de 72 horas tras haberse producido. En caso de que sea el encargado del tratamiento quien sufra la vulneración de seguridad, deberá informar al responsable sin dilación indebida. La notificación de que debe realizar el responsable a la autoridad competente debe contener, entre otras: la naturaleza de la violación de seguridad, las categorías y número de afectados; el nombre del delegado de protección de datos; describir las consecuencias de la violación, así como las medidas adoptadas para remediar la brecha de seguridad. Dada la envergadura de esta obligación, es clara la necesidad de las empresas de invertir en fuertes medidas de seguridad para la protección de datos y en el interés de designar un delegado de protección de datos que se ocupe de centralizar el protocolo de seguridad que la empresa determine al efecto.

5. *El Delegado de protección de datos: funciones y obligaciones*

Junto con el régimen sancionador y el ámbito de aplicación a empresas radicadas fuera de la Unión Europea, el Delegado de protección de datos es la institución jurídica más novedosa del RGPD. Dado que el RGPD establece la responsabilidad proactiva de la empresa y refuerza radicalmente el régimen de garantías en relación con la protección de datos, se exige que las compañías diseñen sus modelos de negocios y todo tipo de acciones que afecten a datos de ciudadanos europeos desde el principio del derecho a la privacidad. La figura del Delegado de protección de datos se convierte así en una **inversión de la compañía** para garantizar que su plan estratégico está alineado con la privacidad. Por este motivo, podemos deducir que, aunque no todas las empresas estén obligadas a tener esta figura, si su modelo de negocio radica de alguna manera en el dato, es aconsejable que la designen porque será quién les ayude a desarrollar su actividad con plenas garantías.

Los arts. 37 (LA LEY 6637/2016), 38 (LA LEY 6637/2016)y 39 del RGPD (LA LEY 6637/2016) nos señalan los mínimos legales de esta nueva institución. Es una figura que puede ser de plantilla o externa, mediante un contrato mercantil a un perfil concreto: especialistas en Derecho con amplia experiencia en protección de datos. El Delegado **goza de ciertos privilegios dentro de la compañía** dado que no puede ser despedido por el ejercicio de sus funciones, es independiente, se sienta en el comité de dirección reportando al más alto nivel jerárquico de la compañía y también reporta directamente a la autoridad competente en materia de datos. Sus funciones principales son: informar de las obligaciones que tienen responsables y encargados; supervisar el cumplimiento del RGPD y formar al personal de la compañía; asesorar y revisar las evaluaciones de impacto; cooperar con la

autoridad de control y actuar como punto de contacto para que cualquier particular le pueda consultar cuestiones relativas a un tratamiento o frente a la autoridad de control.

6. *Nuevo régimen sancionador*

El *CAPÍTULO VIII* del RGPD relativo a los *Recursos, responsabilidad y sanciones* recoge, en sus artículos del 78 al 89 una las más importantes novedades de esta norma en relación con la legislación vigente. El importe de las sanciones a empresas, administraciones y otros entes se eleva de forma exponencial, llegando a alcanzar un importe equivalente al mayor entre **20 millones de euros o el 4% de su facturación anual global.**

Esta multiplicación del importe de las sanciones administrativas es una clara declaración de intenciones del legislador. El objetivo principal, en el desarrollo del RGPD fue el de consagrar el derecho a la protección de datos como un derecho fundamental. Este derecho fundamental deberá regir el diseño de las estrategias empresariales basadas en el dato para poder empoderar al ciudadano en la gestión de los mismos como su legítimo titular.

III. *Principales aspectos del Anteproyecto*

En el RGPD se establece claramente que los Estados miembros podrán elaborar normas internas siempre que sea necesario por razones de coherencia, dentro del sistema normativo nacional, y para que las disposiciones nacionales sean comprensibles para sus destinatarios.

El Anteproyecto está en fase de tramitación parlamentaria y se espera que su aprobación se produzca antes de la plena aplicación del RGPD, el 25 de mayo de 2018. La versión que ahora es objeto de debate complementa el RGPD en los siguientes aspectos:

- Fija la edad de los menores en los 13 años;
- Establecer los criterios bajos los que se deben realizar las evaluaciones de impacto;
- Ofrece un extenso listado tipología de empresas, organizaciones y administraciones obligadas a tener un Delegado de protección de datos;
- Otorga información sobre los códigos de conducta y certificaciones, y
- Matiza y regula detalladamente el régimen sancionador dentro de los límites del RGPD.

Hay otras cuestiones no reguladas en el RGPD que el Anteproyecto contempla como, por ejemplo, los sistemas de exclusión publicitaria (conocidas como «listas Robinson») o los sistemas de información de

denuncias internas en el sector privado. Recordemos que es un Anteproyecto en tramitación y que su contenido puede variar sustancialmente hasta su aprobación final por las Cortes.

IV. *Conclusiones*

El RGPD cambia radicalmente la forma de regular la protección de datos, dando el máximo poder de gestión al titular de dato, el ciudadano europeo, y obligando a empresas, organismos y administraciones a hacer cambios estructurales y organizativos de gran calado para que sean conscientes de que el derecho a la protección de datos es un derecho fundamental.

Esta norma será de aplicación los grandes gigantes tecnológicos radicados fuera de la UE que han construido su modelo de negocio basado en la captación de datos de ciudadanos europeos sin cumplir los estándares de privacidad que la Unión Europea exige.

El RGPD introduce una figura fundamental, el Delegado de protección de datos, que deberá ser incorporado a todas aquellas empresas que, de alguna manera, traten datos a pesar de que el Anteproyecto fija un listado concreto. Esta figura va a ayudar a las compañías y otras entidades a diseñar su estrategia en una política basada en el respecto a la protección de datos y es por ello que ha sido dotada de independencia y del máximo nivel jerárquico. El Delegado de protección de datos es una figura externalizable. Es aconsejable que el Delegado sea una persona que conozca su empresa a la perfección y con un nivel de interlocución y conocimiento de los procesos muy alto. Sin perjuicio de lo anterior, puede delegar la mayoría de las tareas que debe desempeñar en despachos de abogados especializados en protección de datos.

El RGPD permite que los Estados miembros elaboren leyes nacionales sólo en la medida en que completen y/o aclaren su tenor. En España, estamos en proceso de tramitación del Anteproyecto. En cualquier caso, el 25 de mayo será de plena aplicación el RGPD y las empresas que no se hayan adecuado a la norma están expuestas a cuantiosas sanciones administrativas. Dado que la adecuación al RGPD implica un proceso que conlleva varios meses de trabajo, las asociaciones de profesionales de la privacidad recomiendan que no demoren dicha adecuación a 2018.