PONENCIA

El Reglamento General de Protección de Datos (RGPD).

El Reglamento europeo 679/2016 o Reglamento General de Protección de Datos (RGPD) mantiene, en general, los fundamentos de protección de datos que ya establecía la Ley Orgánica 15/1999 (LOPD) y su Reglamento de Desarrollo aprobado por Real Decreto 1720/2007, aunque introduce algunas novedades y matices.

D. ANDRÉS CALVO
Responsable de la Unidad de Evaluación y Estudios Tecnológicos de la AEPD

La primera de estas novedades es que no estamos hablando de una Directiva como ocurría con la Directiva de protección de datos 95/46 sino de un reglamento de aplicación directa y que, tras dos años de *"vacatio legis"*, será plenamente aplicable a partir del próximo 25 de mayo de 2018. Por lo tanto, no existirá trasposición de la norma a cada uno de los estados miembros, la norma será aplicable directamente en todos ellos y durante este periodo los estados no podrán hacer uso de normas que sean contrarias a los principios del RGPD.

En definitiva, hablamos de una norma de aplicación directa que desplaza a las normas nacionales en materia de protección de datos y que permite cierta capacidad a los estados miembros para regular aquellas cuestiones de índole regional que pudieran quedar fuera de este nuevo marco regulatorio europeo.

El hecho de que no exista una Directiva sino un Reglamento directamente aplicable, debe entenderse como un intento de armonización de la normativa de protección de datos, evitando la posibilidad de distintas interpretaciones de la norma según su trasposición en cada uno de los estados miembros. El RGPD representa un esfuerzo de armonización de las normas europeas de protección de datos que obligan al establecimiento de mecanismos de coordinación y regulación entre autoridades de protección de datos europeas, coordinación que se sustentará en la figura del Comité europeo de protección de datos (actual Grupo de trabajo del artículo 29 de la Directiva 95/46).

Tal vez la novedad más importante que aporta el nuevo RGPD es el principio de

responsabilidad activa por el que los responsables deben cambiar su papel reactivo, corrigiendo los errores y defectos de los tratamientos de datos, hacia un enfoque proactivo en el que los riesgos y posibles errores se evalúen por adelantado y se mitiguen antes de que tengan lugar. Al igual que la LOPD, el RGPD obliga a los responsables de los tratamientos de datos a aplicar las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos, pero además incluye la obligación de los responsables de estar en posición de demostrar en todo momento que las condiciones en las que se realizan los tratamientos de datos personales incluyen una constante puesta al día de las medidas de seguridad con respecto a las situaciones de riesgo específicas de cada tratamiento.

Desde un punto de vista práctico este enfoque de riesgos del RGPD, además del tradicional enfoque de riesgos encaminado a determinar las medidas de seguridad para garantizar el apropiado funcionamiento de los sistemas de información o los riesgos de negocio, añade una tercera componente: los riesgos para los derechos y libertades de las personas. Este enfoque puede suponer para los responsables una aparente línea de separación entre los riesgos que les afectan directamente a ellos y los que afectan a terceros.

Pero el enfoque de riesgos no se limita a una constante revisión de los riesgos, sino que a esto habría que añadir los principios de protección de datos desde el diseño, protección de datos por defecto, y las evaluaciones de impacto. Se trata de evaluar y mitigar riesgos para los derechos y libertades de las personas que pudieran derivarse de los tratamientos de datos personales en función de las circunstancias concretas de cada tratamiento e incluso con anterioridad a estos (evaluaciones de impacto).

En línea con el papel proactivo de los responsables del tratamiento, el RGPD añade algunas obligaciones a los responsables como son la elaboración y mantenimiento de un registro de actividades de tratamiento. Esta obligación recuerda en cierta medida a la obligación de inscripción de ficheros derivada de los artículos 20 y 26 de la LOPD y que, de alguna manera, puede entenderse como el punto de partida desde el que, como responsables, podemos empezar a elaborar el registro de actividades de tratamiento.

“Se trata de evaluar y mitigar riesgos para los derechos y libertades de las personas que pudieran derivarse de los tratamientos de datos personales en función de las circunstancias concretas de cada tratamiento e incluso con anterioridad a estos.”

El RGPD incorpora la figura del Delegado de Protección de Datos (DPD) sobre quien recae la responsabilidad de asesorar al responsable para que los tratamientos de datos se realicen de acuerdo a los principios del reglamento. Aunque esta figura es de nueva creación, el papel que representa ya venía siendo realizado en alguna medida por los responsables de protección de datos o por asesores y consultores, y en cierta forma supone una regularización de estas actividades. La figura del DPD no está asociada a ninguna especialidad académica concreta ni a ninguna profesión específica, es un perfil multidisciplinar que incorpora conocimiento de negocio, conocimientos técnicos y conocimientos jurídicos de protección de datos. El carácter multidisciplinar de esta figura hace difícil aglutinar todas las competencias en una única persona, posiblemente en algunas ocasiones este profesional realizará labores de asesoramiento y coordinación de las actividades encaminadas a garantizar la licitud de los tratamientos de datos personales y según su perfil requerirá en ocasiones tanto apoyo técnico como apoyo jurídico. El DPD podrá ejercer sus funciones a tiempo completo o compaginar esta actividad con otras actividades, en este último caso será conveniente tener en cuenta que a la hora de designar al DPD los responsables deberán realizar un análisis de los posibles conflictos de intereses que impidan al DPD realizar su función de forma independiente.

La aplicación del RGPD implicará la obligación de todos los responsables de los tratamientos de datos personales de notificar las violaciones de seguridad a la autoridad de control correspondiente. Hasta la fecha las obligaciones de notificar derivaban de la Ley General de las Telecomunicaciones que convertía a los proveedores de servicios de comunicaciones en sujetos obligados a notificar las violaciones de seguridad, pero a partir del 25 de mayo de 2018 esta obligación será aplicable a cualquier responsable de un tratamiento de datos personales quien además deberá también comunicar de la violación de seguridad a los interesados.

“Finalmente, habría que subrayar entre las novedades que introduce el RGPD, el principio de transparencia por el que los responsables deben de facilitar a los interesados información concisa, inteligible, de fácil acceso y en un lenguaje claro y sencillo.”

Otra de las cuestiones a destacar en cuanto a las novedades del RGPD es la relación entre el responsable del tratamiento y el encargado o subencargado. En el reglamento se establece el deber de diligencia del responsable y la posibilidad de supervisión al encargado del tratamiento. Así, la relación responsable-encargado implica deber de diligencia, proactividad y supervisión por parte del responsable.

Finalmente, habría que subrayar entre las novedades que introduce el RGPD, el principio de transparencia por el que los responsables deben de facilitar a los interesados información concisa, inteligible, de fácil acceso y en un lenguaje claro y sencillo, principio que adquiere especial importancia en el caso de los menores.

Para más información puede consultarse el microsite que la Agencia Española de Protección de Datos ha creado con el fin de aglutinar toda la información que pueda ser de ayuda a los responsables en su adecuación al RGPD, guías, recomendaciones, herramientas, dictámenes, etc. ✱