# Entender el nuevo marco regulador de protección de datos, ¿amenaza u oportunidad?

Por Daniel Gómez
Director Organización
Andbank

En la actualidad, las empresas y las organizaciones públicas adquieren e intercambian un volumen creciente de información incluyendo, entre otros, los datos personales de los usuarios.

El adelanto tecnológico de los últimos años ha conducido la evolución digital en la relación empresa-cliente, pero a la vez ha incrementado significativamente los riesgos y amenazas de seguridad, dejando patente la necesidad de establecer un nuevo marco legislativo que vele por la privacidad y por la protección de los datos personales.

El 24 de mayo de 2016, la Unión Europea (UE) publicó el nuevo Reglamento General de Protección de datos (RGPD), que entrará en vigor el 25 de mayo de 2018 en toda la UE, sustituyendo la regulación actual que se aplicó hace 20 años.

El reglamento introduce un marco homogéneo en el ámbito comunitario, que define las reglas de actuación para cualquier empresa privada o entidad púbica que gestione datos personales de ciudadanos de la UE, indistintamente del lugar donde se encuentren, y con independencia que se traten de clientes, empleados o contactos.

El principal objetivo que persigue esta nueva regulación es recuperar el control sobre los datos propios como un derecho fundamental de toda persona física.

**Principales pilares del nuevo marco normativo**

El nuevo reglamento se puede resumir en la evolución de una serie de aspectos clave sobre el marco actual.

En primer lugar, se amplía el concepto de dato personal a cualquier información que permita relacionar o identificar la persona e incorpora nuevos tipos como son la localización geográfica, datos biométricos y genéticos, las fotografías o, incluso, el chip de identificación de la mascota.

Así mismo, se amplían los derechos del ciudadano respecto al control de los datos propios: (i) limitación en el procesado de datos (ii) olvido, que permitirá requerir la eliminación de sus datos, y (iii) portabilidad, que permitirá la extracción de los datos para llevarlos a otra entidad.

Complementariamente, se introduce la obligación de obtener un consentimiento expreso e inequívoco para los tratamientos de datos que realice la empresa para fines propios. Esto comporta, por lo tanto, definir una política informativa para facilitar el consentimiento, que sea de fácil entendimiento y accesibilidad, que explique para qué usos se usarán los datos, quienes tendrán acceso y por cuánto tiempo se custodiarán.

Otra medida relevante será la obligación de designar un responsable de protección de datos (DPO, Data Protection Officer). Las funciones de este nuevo rol van más allá de las del actual responsable de datos, dado que tendrá que asesorar a la entidad, estableciendo las medidas técnicas y organizativas apropiadas para garantizar las obligaciones, y supervisar su cumplimiento. El DPO actuará como enlace con las autoridades de control y, entre otras obligaciones, tendrá que notificar todo compromiso de seguridad en un plazo máximo de 72 horas. Se estima que en todo el territorio de la UE se necesitarán unos 28 mil DPO.

**... la amenaza...**

La adopción de todas estas medidas supondrá un reto en sí mismo para cualquier entidad. Pero más allá, una de las principales motivaciones será evitar las cuantiosas sanciones en caso de infracción de la normativa. Las entidades se enfrentarán a multas de un máximo de 20 millones €, o un 4 % del volumen de negocio total anual, aplicando el importe de mayor cuantía.

Ejemplos muy recientes del que podrá ser la exigencia son las sanciones que la Agencia Española (AEPD) ha establecido a empresas como Whatsapp o Facebook por no haber comunicado a los usuarios los usos que se harían de sus datos y hacer uso para fines propios sin haber obtenido un consentimiento explícito. Si bien la sanción actual, 300 mil €, seguro que no resultará material para estas grandes corporaciones, establece una clara advertencia.

**... y la oportunidad de transformar**

La severidad de las sanciones obliga a las entidades a revisar totalmente todos sus procesos de negocio y de sistemas de información, para incorporar el dato como un requerimiento más en la definición.

El gobierno de los datos abrirá un nuevo abanico de oportunidades, tanto en torno a la monetización del dato como en el ofrecimiento de servicios relacionados con los derechos de los ciudadanos. Generar la confianza permitirá fidelizar el cliente, pero a la vez una inteligencia más grande sobre sus preocupaciones e intereses, que pueden favorecer a determinar los productos y servicios que mejor encajan con sus necesidades. Medidas como la portabilidad de los datos fomentarán la desintermediación y la libre competencia entre empresas.

Por lo tanto, la adopción del RGPD, así como otras recientes normativas europeas como el PSD2 (Directiva de servicios de pago), no dejan de ser dinamizadores de la evolución y de la transformación digital en los modelos de negocio, la eficiencia operativa y la experiencia de cliente.