¿Cómo nos afecta la nueva protección de datos?

Llevas una semana recibiendo sin parar correos electrónicos anunciando la "nueva política de privacidad" de tiendas donde has comprado al menos una vez. ¿Cómo te afecta? El pasado 25 de mayo entró en vigor el nuevo Reglamento General de Protección de Datos (RGPD). Aunque este reglamento fue aprobado en abril de 2016, no ha sido hasta hace unos pocos meses, o incluso semanas, cuando hemos empezado a ser conscientes de sus implicaciones. Al igual que en España tenemos la Ley Orgánica de Protección de Datos Personales (LOPD) también existen legislaciones similares en otros países de la Unión Europea. El RGPD se ha diseñado para unificar tanto las definiciones relacionadas con los datos personales como los criterios para su protección.

Con la RGPD, denegar los permisos deberá ser tan fácil como aceptarlos. / John Loo.

El objetivo principal del RGPD es permitir a cada ciudadano (persona física) tener más control sobre la información personal que tengan sobre ella tanto empresas privadas como organismos públicos, manteniendo el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

Este control se articula en los siete derechos que recoge el nuevo reglamento, que amplían los ya conocidos derechos ARCO de la LOPD. Esto es, además de los derechos de Acceso, Rectificación, Cancelación y Oposición, se añaden los derechos a la limitación del tratamiento, a la portabilidad de los datos y a no ser objeto de decisiones automatizadas. El derecho de cancelación se sustituye por el derecho al "olvido".

En la práctica estos derechos implican, en primer lugar, que al facilitar nuestros datos personales a una organización, tenemos que dar nuestro consentimiento explícito y separado del resto de consentimientos, a cada uno de los tratamientos que se vayan a realizar con nuestra información. Por ejemplo, podemos indicar al banco que puede tratar nuestros datos para cumplir con el contrato que tenemos con ellos, pero no para realizar acciones comerciales. Otro aspecto relacionado con éste, es que el denegar los permisos deberá ser tal fácil como aceptarlos.

Siempre con excepciones y, entre otras cosas, el ciudadano va a poder solicitar de forma sencilla a la organización que los trata, qué datos personales tiene sobre él, para qué los tiene y su modificación si no son correctos. También tienen que permitir al ciudadano solicitar su eliminación en determinados casos e informar al ciudadano si sus datos se utilizan para tomar decisiones automatizadas, como las utilizadas para predecir el rendimiento en el trabajo, la situación económica o cuestiones de salud, pudiendo denegar esa toma de decisiones automáticas. Por último, el derecho a la portabilidad permitirá a los ciudadanos exportar en un formato estructurado los datos personales que tenga una organización para transmitírselos a otra.

Una vez que un ciudadano ejecuta alguno de sus derechos, las organizaciones dispondrán de un período de tiempo definido para hacerlos efectivos. En general, el RGPD da de plazo un mes, ampliable según el caso por otros dos más.

De cara al organismo que trata los datos, la principal diferencia con la LOPD (que tendrá que adaptarse al nuevo reglamento) consiste en que la LOPD categoriza la información personal en tres niveles: bajo, medio y alto, indicando de forma precisa las medidas de seguridad a aplicar en cada caso para proteger esta información. En el caso del RGPD la información no viene categorizada, lo que aumenta el rango de lo que se considera dato personal, ni por lo tanto se indican las medidas a aplicar en cada caso. Cada organización debe, en función de un análisis de riesgos, determinar el valor de la información y las medidas de protección adecuadas. Será responsabilidad de la organización hacerlo de forma adecuada. Como medidas de protección el RGPD únicamente incluye explícitamente dos de ellas, que son el cifrado de la información y la pseudo-anomización de los datos.

En caso de que se produzca un incidente de seguridad la nueva ley obliga a las organizaciones a notificar cualquier fuga o infracción de datos detectada en las siguientes 72 horas. También aumentan las multas por incumplimiento.

Luis Javier García Villalba es investigador del departamento del Ingeniería de Software e Inteligencia Artificial.