



Publicado el Código de Buenas Prácticas en protección de datos para proyectos de “Big Data”

El Código, preparado por la Agencia Española de Protección de Datos e ISMS Forum Spain, identifica las principales cuestiones prácticas a tener en cuenta cuando se manejen datos a gran escala

El término “Big Data” puede definirse como el conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzadas hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo.

Uno de los usos principales del Big Data es el establecimiento de correlaciones y elaboración patrones o perfiles de consumidores (profiling). Tiene especial interés en innumerables sectores en los que se lleva a cabo la venta por internet, e incluso en la venta presencial, a través de las llamadas “tarjetas de fidelización”, que permiten conocer los hábitos de compra de un ingente número de consumidores. El Big Data también es una herramienta eficaz en sectores como el sanitario, donde existen ya muchos ejemplos de su eficacia, por ejemplo para reducir los tiempos de ingresos hospitalarios, o para predecir futuras enfermedades y riesgos sanitarios.

Pese a las grandes ventajas que puede comportar, el Big Data también plantea evidentes riesgos cuando se contienen datos personales. Piénsese, por ejemplo, en el uso indiscriminado de tales datos sin preservarse adecuadamente la privacidad de las personas, o sin adoptarse las medidas de índole jurídica, organizativa o técnica que resulten precisas. El Código da unas pautas de actuación para minimizar o eliminar dichos riesgos en tales proyectos, en línea con lo dispuesto en el nuevo Reglamento Europeo de Protección de Datos, que será aplicable en Mayo de 2018.

Principios básicos

El Código recomienda considerar la privacidad desde el diseño (Privacy by Design), con el objetivo de asegurar que las garantías de protección de datos se incorporan ya desde la fase inicial de planificación del proyecto. Asimismo, promueve la autorregulación por parte de las empresas que gestionen proyectos de Big Data, mediante la elaboración de códigos de conducta en la materia (Accountability). También exige la realización de evaluaciones de impacto para valorar los posibles riesgos, entre otros, en aquellos casos en los que se manejen datos relativos a la salud.

Aspectos legales y técnicos

Sobre la base de los riesgos que originan estos tratamientos para la privacidad de las personas, el Código identifica aquellos aspectos que deben ser abordados para que los proyectos de Big Data sean conformes a la normativa sobre protección de datos. Por una parte, trata los aspectos legales más relevantes a considerar, como la transparencia en la información previa facilitada a los afectados, o la obtención del consentimiento y el ejercicio de derechos por dichos afectados, o qué sucede con usos posteriores, no previstos cuando se obtuvo el consentimiento informado. Por otra parte, el Código revisa las diferentes cuestiones técnicas y de seguridad a tener en cuenta en estos proyectos. En concreto, identifica las estrategias de privacidad más usuales: anonimización, cifrado, control de acceso y trazabilidad.