

## Los retos de la privacidad frente a la globalización, el avance tecnológico y la penetración de las TI en la sociedad

El principal reto regulatorio para la privacidad reside en establecer un justo balance que garantice el respeto del derecho a la protección de datos de los ciudadanos sin imponer barreras para el desarrollo de la sociedad de la información, y en especial, de servicios como las redes sociales, *cloud computing* y los motores de búsqueda en Internet.

En cualquier caso, la privacidad constituye un valor en alza para las organizaciones. El respeto del derecho a la protección de datos de los ciudadanos se traduce en el incremento de la confianza en las organizaciones, y la confianza repercute en la fortaleza económica y en la reputación de estas. Asimismo, la responsabilidad social corporativa forma, sin duda, parte del activo de las compañías. La confianza es un elemento diferenciador en el mercado. Por una parte, los ciudadanos cada vez son más conscientes de sus derechos, y cuidadosos con las entidades a las que confían sus datos personales. Por otro lado, la ocurrencia de un incidente de seguridad, o el incumplimiento de la normativa vigente en materia de protección de datos, además de producir pérdidas directas por la posible imposición de sanciones administrativas y condenas judiciales de indemnización, afectan directamente al valor bursátil de la empresa, y causan daños a la reputación de la marca.

### COMPROMISO DE LA ALTA DIRECCIÓN

Por todo ello, necesitamos fomentar la cultura de la privacidad. En España, el grado de cultura sobre protección de datos y privacidad varía mucho en función del tamaño de las organizaciones. Muchas de las grandes compañías han alcanzado un nivel de

*“Muchas de las grandes compañías han alcanzado un nivel de madurez importante en materia de protección de datos”*



Nathaly Rey\*

*“La seguridad de la información y el cumplimiento normativo constituyen algunas de las principales barreras para la implantación de ‘cloud’ por parte de las organizaciones”*

madurez importante en materia de protección de datos. El punto de partida para ello, es sin duda, el compromiso de la alta dirección con la privacidad. Esto luego se traduce en políticas, procedimientos y controles, enmarcados bajo el paraguas de GRC, en la figura del DPO (Data Privacy Officer) como máximo responsable, reportando a un nivel alto dentro de la compañía, y en la existencia de departamentos de protección de datos, que aglutinan conocimientos técnicos, jurídicos y de gestión de riesgos propios de la función. En el caso de las pequeñas y medianas empresas y autónomos (más del 99% del total del tejido empresarial español), lo tenemos más complicado, estamos lejos de una madurez en materia de protección de

datos, es por ello que cobran especial relevancia las iniciativas destinadas a la concienciación y el fomento del cumplimiento de la normativa.

### ‘CLOUD COMPUTING’

#### Y REDES SOCIALES, LOS GRANDES DESAFÍOS

El *cloud computing* se perfila como un modelo disruptivo que cambiará la forma de entender la informática por parte de los usuarios y que permitirá la realización de la tan esperada eficiencia de costes en el entorno tecnológico empresarial, al brindar a las organizaciones la posibilidad de acceder a un gran número de recursos informáticos y de disponer de una enorme capacidad de procesamiento y almacenamiento, sin necesidad de instalar infraestructuras localmente, ni de invertir previamente en licencias de software, orientando siempre los costes a los recursos efectivamente utilizados. Sin embargo, la seguridad de la información y el cumplimiento normativo, especialmente en materia de protección de datos personales, constituyen unas de las principales barreras para la implantación de este tipo de servicios por parte de las organizaciones. Las preocupaciones relacionadas con estos dos factores están más que justificadas, teniendo en cuenta que la implantación de servicios de cloud podría implicar que un tercero llegue a controlar, almacenar o procesar en sus servidores, y de forma deslocalizada, activos de información sobre los que recaen numerosas obligaciones en materia de privacidad, y que son muy valiosos para el negocio. Por su parte, en el entorno de las redes sociales, los usuarios deben tener la posibilidad de ejercer efectivamente su derecho a la autodeterminación informativa en las redes sociales, esto quiere decir que las configuraciones de privacidad deben ser sencillas, accesibles y transparentes. Y por supuesto, deben estar restringidas al máximo por defecto.

\* Nathaly Rey es directora general de la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain.