08 de febrero de 2017 | 01:03

LEGALTODAY

POR Y PARA ABOGADOS

Blog ECIJA 2.0

8 de Febrero de 2017

Diego Pérez

asociado de IT de ECIJA

¿Qué coste (reputacional) tiene para una empresa sufrir un ciberataque?

La mayoría de las empresas amplían año tras año su inversión en seguridad de la información. No obstante, cuando una empresa sufre un ciberataque se ponen de manifiesto las debilidades de éstas en un mundo hiperconectado y globalizado como el actual.

Los casos más relevantes siguen dando que hablar a día de hoy. Compañías como Yahoo!, Ashley Madison o Tesco Bank se han visto obligadas a adecuar sus procedimientos y políticas para recuperar la confianza de los mercados dañada tras los incidentes sufridos. **Junto con las sanciones en las diferentes órdenes e indemnizaciones millonarias,** las vulneraciones de seguridad en tanto afectan a la confidencialidad de la información, implican un coste reputacional difícilmente cuantificable, y el otorgamiento de una ventaja al resto de competidores en su sector.

En un momento en que la economía digital ha evidenciado el conocimiento, no sólo de las necesidades del cliente, sino de los potenciales clientes, los datos personales se han erigido como dovela central del sistema empresarial. Un mayor conocimiento de las personas **posibilita evolucionar los productos que las entidades ofrecen hasta la personalización** casi total o el diseño de servicios que cubran las necesidades específicas del cliente, la aplicación de análisis masivos de datos facilita a las empresas la explotación de la información que tienen, optimizando sus procesos y recursos, haciendo más rentables los modelos de negocio y mejorando la experiencia del usuario.

Junto con estos beneficios, la adopción de medidas de seguridad que garanticen la confidencialidad de la información, su integridad y la imposibilidad de accesos **(mal intencionados o no)** por parte de terceras personas, conllevan indudablemente un factor decisivo para la generación de confianza en la empresa, tanto por parte de los propios empleados, como de clientes y potenciales clientes. Aspectos clave en casi la totalidad de los sectores, pero especialmente en aquellos **que desarrollan su actividad en mercados financieros, banca, salud, derecho u otros servicios** en que se trata información de carácter personal.

Actualmente, nuestra normativa enumera una serie de obligaciones y estándares que deben ser adoptados por las empresas, en relación con el tratamiento y explotación de los datos de clientes o potenciales. **Obligaciones que el Reglamento Europeo**, en vigor y de plena aplicación en el primer semestre de 2018, evoluciona a la adopción de garantías y medidas de seguridad hacia la implementación de mecanismos proactivos y el diseño de productos y soluciones respetuosos con la privacidad desde el diseño de los mismos.

De igual manera, **en el momento de actuar ante un incidente de ciberseguridad,** tal y como hemos aprendido de los diferentes ejemplos que hemos comentado, debemos tener en cuenta que, junto con los niveles de seguridad que recoge nuestra normativa actual de protección de datos, **o las categorías que consolida el Reglamento Europeo,** existe un nivel de seguridad no recogido en nuestra normativa que afecta a la expectativa que el propio usuario tiene de su privacidad e información o el impacto que una fuga de determinada información puede tener para éste. Así las

cosas, **este nivel social de protección de datos,** implicarían que a un dato de nivel básico se le deberían aplicar mayores medidas de seguridad.

Uno de os aspectos que la nueva norma europea democratiza es la comunicación de brechas de seguridad. Utilizamos el término democratizar, en el sentido de la extensión de una obligación que ya era exigible a las empresas de telecomunicaciones, **conforme a nuestra actual Ley General de Telecomunicaciones,** al resto de entidades, implementando, junto con la comunicación a la Agencia Española de Protección de Datos o autoridad de control nacional, la remisión de información a los propios afectados. Un hecho que, si bien gestionado puede minimizar el riesgo reputacional de la empresa, **en el caso contrario puede tener un gran impacto en las cuentas y número de clientes de la misma,** así como en la propia imagen corporativa y por tanto, en su modelo de negocio, afectando incluso a la viabilidad del mismo.

Por último y no menos importante, debe recordarse que la utilización de la información objeto de la fuga o de la vulneración de las medidas de ciberseguridad, en tanto pertenecería a la esfera íntima del afectado, **no sólo podría implicar una intromisión ilegítima en el derecho a la intimidad del propio usuario sino que,** podría incluso afectar a la intimidad de su entorno más próximo.