

El pitorreo

Muchos aún recordamos el famoso pitorreo de hace unos años cuando Zapatero fue transmutado –*defacement* mediante– en un afamado comediante británico durante el estreno digital del sitio web oficial de nuestra copresidencia europea. El elevado impacto mediático de la broma y el subsiguiente sonrojo por no haber ‘securizado’ convenientemente el sitio web, fueron considerables. Aunque, eso sí, sin mayores consecuencias ni lecciones aprendidas.

Por el contrario, y al albur del recalentado ambiente internacional por las acciones de Estado Islámico y Corea del Norte, otra reciente ‘desfiguración’, acontecida hace solo escasas semanas en EE.UU., sí parece que irá a mayores. Me refiero al *defacement* causado en las cuentas de Twitter y YouTube del Mando Central del Ejército norteamericano, en las que simpatizantes de El insertaron provocadoras amenazas de un inquietante ‘CiberCalifato’. Si bien la incursión cibernética en sí tampoco revistió gravedad, por el contrario su alcance mediático fue demoledor pues sucedió precisamente cuando el mismísimo Barack Obama se dirigía a su nación para anunciar nuevas y más ambiciosas medidas de ciberseguridad destinadas a proteger el ciberespacio estadounidense y dotar de más confianza a una sociedad ya conectadísima.

La anécdota no es baladí pues precisamente el paquete de medidas anunciadas por el ejecutivo norteamericano para su evaluación y promulgación plantean importantes retos, encaminados todos ellos a combatir cualesquiera ciberamenaza y ciberdelito que erosionen el normal funcionar digital y a cimentar la protección de Estados Unidos dentro de sus fronteras físicas y virtuales ante atentados contra su soberanía.

Así, la unificación legislativa estatal relativa a fugas y quiebras de información (plazo de notificación, sanciones...), una tipificación más granular de los ciberdelitos (p.e., venta de *spyware* y *malware*, tráfico de redes zombi, *botnets*...), el cerco al mercadeo de datos personales y, cómo no, la ley que concederá a los consumidores el derecho a decidir qué información personal se recoge de ellos y cómo la usan, son, si duda, hitos decisivos de unas medidas encaminadas a clarificar una dimensión de contorno digital aun excesivamente difuso y a advertir al lado oscuro que su impunidad tiene los días contados.

La batalla está pues librándose en muchos frentes. El perfilado de lo que va a ser la privacidad que marcará nuestro devenir digital, las exigencias de no desinhibirse y hacer bien los deberes a la hora de proteger los activos de información empresariales evitando las brechas (el *affaire* de la reincidente Sony ha sido paradigmático), y combatir un cibercrimen más profesionalizado que nunca, son desafíos a los que la administración Obama confiere una criticidad nuclear.

Estas prometedoras medidas, a pesar de haber sido lastimeramente empañadas por los recientes escarceos, no lograrán que EE.UU. ceje en su empeño de sacarlas adelante. Y deberían servir de acicate para que también desde Europa apretemos más el acelerador, espabilando y afrontando las cuitas digitales con bastante más decisión y medios de los habidos hasta ahora. Precisamente, el Acuerdo de Libre Comercio con nuestros aliados estadounidenses no acaba de fraguar por, entre otros temas, la espinosa delimitación de una privacidad agresivamente zarandeada por aquellos. Y el nuevo Reglamento Europeo de Protección de Datos, con su polémico 3%/5% de la facturación por sanción causada por fuga, parece que aplaza su desembarco todavía a un par de años vista.

Todo indica que los ciberpitorreos y las ciberagresiones, en tropel, van a seguir a la orden del día. Y también que si estos actos siguen proliferando, como así parece, tal vez la sociedad por hartura acabe infravalorándolos e ignorándolos. Va a librarse una batalla feroz que solo acaba de comenzar y más nos valdrá que la justicia acabe por desperezarse y entienda que la naftalina ya no es suficiente y que debe enfundarse una toga más acorde, la del siglo XXI. ●



LUIS G. FERNÁNDEZ
Editor
lfernandez@codasic.com