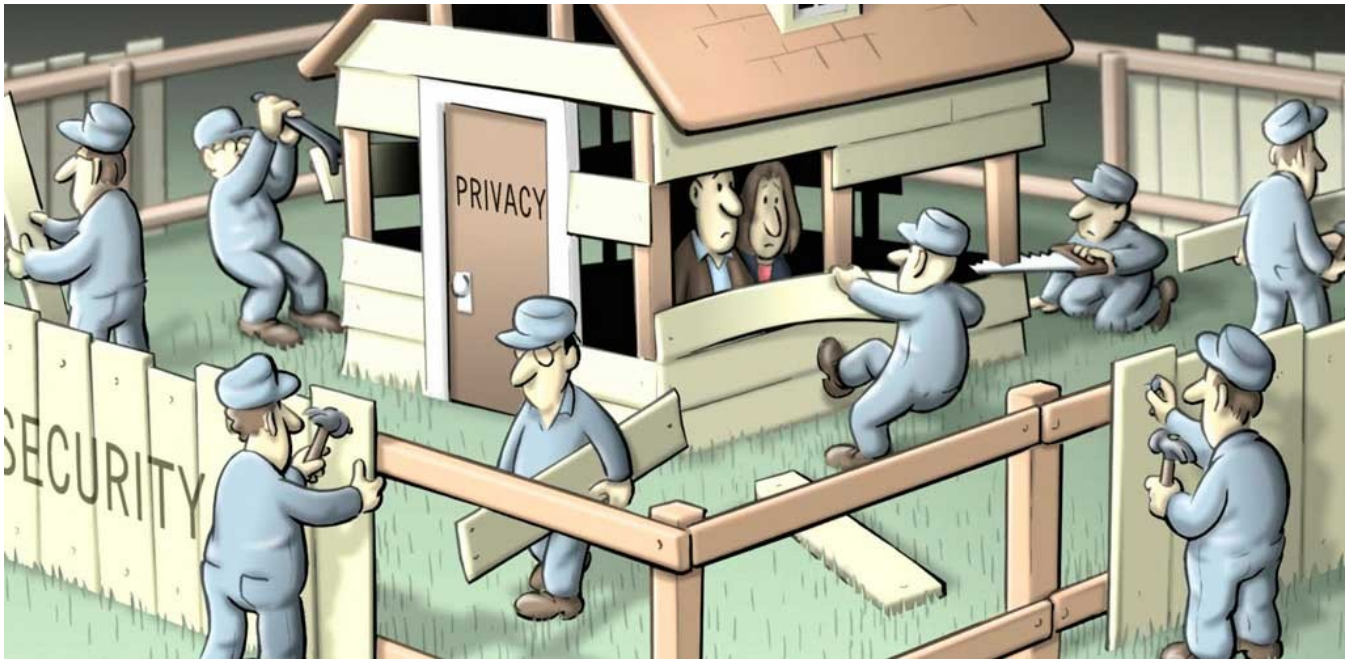
Privacidad vs Seguridad



Si os digo la verdad, lectores míos, en este segundo post no pensaba hablar sobre el eterno debate entre la seguridad y la privacidad, pero ayer tuve la oportunidad de asistir a una conferencia que se realizaba en la biblioteca de nuestra universidad sobre ciberseguridad, y no me lo he pensado dos veces. Tarde o temprano quería introduciros este gran dilema, y ¿qué mejor momento que ahora que la mayoría de compañeros asistieron al evento?

La Fundación Innovación Bankinter lanzó la XXV publicación del Future Trends Forum, donde se analizó una de las tendencias de innovación: la ciberseguridad, planteándola como el arma para luchar contra los retos que plantea la seguridad en la era digital y donde los expertos del FTF plantean una hoja de ruta con diez propuestas dirigidas a regular y mejorar nuestra ciberseguridad. [1] [2]

La ciberguerra, el ciberespionaje, la vigilancia masiva son amenazas actuales

a las que se suman y se sumarán otras. Más allá del infinito mundo de ventajas que ha supuesto Internet, nuevos escenarios se presentan en el ciberespacio: posibles conflictos bélicos ejecutados con armas autónomas o entre máquinas y hombres, o grandes sabotajes contra infraestructuras críticas de los países.

Es por estas y otras situaciones que llegamos a plantearnos ciertas cuestiones: "*¿Está bien pedirles a las empresas de tecnología que violen la privacidad de sus usuarios por motivos de 'seguridad nacional'?*" "*¿Se justifica que todos los usuarios de Internet entreguemos nuestro derecho a la privacidad si eso puede evitar un ataque terrorista y salvar vidas?*" [3]

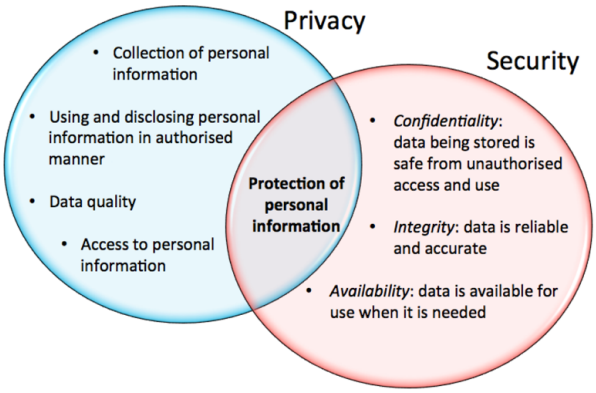
Si bien es cierto que llevamos tiempo haciéndonos ese tipo de preguntas, en este año, está siendo más urgente que nunca por varias razones. En primer lugar, el mundo occidental se siente amenazado por un grupo islamista para el que Internet no es un lugar extraño. Lo usa para reclutar, hacer propaganda y comunicarse, utilizando las mismas herramientas que el resto del mundo. Por otra parte, los ciudadanos somos cada vez más conscientes de que nuestra privacidad en Internet es importante y está en riesgo. Desde el escándalo de Snowden [4], sabemos que los gobiernos del mundo quieren tener acceso a todo lo que viaja por Internet. Por último, en breve se realizarán las elecciones a la presidencia en Estados Unidos. Los asuntos tecnológicos de ese país tienen repercusión mundial, ya que los servicios más usados en el mundo son de allí y las discusiones estadounidenses sobre regulación tecnológica tienden a replicarse en el resto del mundo.

Es verdad que, situaciones preocupantes, como la del primer caso, representan un contexto único donde la privacidad es más probable que sea una de las menores preocupaciones personales. En teoría, las actividades de rastreo no deben provocar ningún tipo de preocupación por la privacidad cuando estas actividades se utilizan específicamente para fines de seguridad. Sin embargo, el problema no proviene de esta utilización específica destinada a fines de advertencia pública o seguridad personal. El problema viene de que la disponibilidad ininterrumpida de tecnologías de rastreo esté en manos del gobierno, utilizándose en el día a día. [5]

Y es que la información de ubicación es un tipo de información personal que puede tener graves consecuencias sobre la privacidad de un individuo si se usa mal. Este tipo de información puede ser recopilada, almacenada, agregada y cuando se correlaciona con otra información personal, se puede crear una visión amplia de los patrones de comportamiento o retratos detallados de los

hábitos individuales. El uso de este tipo de sistemas plantea preocupaciones sobre la privacidad en general, así como los temores de llegar a ser un objetivo sospechoso.

El tolerar prácticas que atenten a la privacidad de los ciudadanos, sin un claro control, no favorece la seguridad. Al contrario, puede que la perjudique. Y esto, que es tan claro para el individuo, se está viendo claro en la sociedad.



Puede que tengamos que cambiar un poco el chip y dejar de ver a la privacidad como un costo de la seguridad, y empezar a verla como un beneficio. No se trata de privacidad contra seguridad, sino de que la privacidad Es seguridad y deben ir de la mano una con la otra.

REFERENCIAS

[1] Bankinter, F. (2016). *Ciberseguridad: un desafío mundial*. Blog.bankinter.com. Disponible en: https://blog.bankinter.com/economia/-/noticia/2016/5/5/ciberseguridad-innovacion-fundacion-bankinter [Consulta 3 Nov. 2016].

[2] WOLFF, E., Vivienda, S., Orbyt, E., Farmacéutico, C., Médico, D., Búho, E., Señor, R., Editorial, E., Editorial, U., Empleo, E. and Editorial, E. (2016). *Seguridad cibernética vs privacidad: cómo fomentar la confianza*. ELMUNDO. Disponible en: http://www.elmundo.es/economia/2016/05/27/574810c346163f9c5d8b45bf.html [Consulta 3 Nov. 2016].

[3] ENTER.CO. (2016). *Citar un sitio web – Cite This For Me*. Disponible en: http://www.enter.co/chips-bits/seguridad/lo-que-va-a-pasar-en-2016-privacidad-vs-seguridad/ [Consulta 3 Nov. 2016].

[4] Blusiewicz, J. (2016). *The Case of Edward Snowden: A Different Path*. Inquiries Journal. Disponible en: http://www.inquiriesjournal.com/articles/1196/the-case-of-edward-snowden-a-different-path [Consulta 3 Nov. 2016].

[5] Ieeexplore.ieee.org. (2016). *IEEE Xplore Document – Privacy vs. Security in National Emergencies*. Disponible en: http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6163994 [Consulta 3 Nov. 2016].