


[Portada](#)
[Secciones](#)
[Archivo](#)
[Oficina de Comunicación](#)
[Links](#)

Campus Digital Noviembre 2013



Criterios

0% privacidad y 0% seguridad, 100% vigilancia electrónica

Edgar Vega Briceño (*)

¿Recuerdan la película [Matrix](#)? La trama asume la existencia de un mundo controlado por máquinas y agentes de software que saben todo lo que hacemos y pensamos. Pues bien, en los últimos meses se ha desatado una masiva onda de mensajes sobre las prácticas de vigilancia electrónica efectuadas por la Agencia de Seguridad Nacional de los Estados Unidos, que no dista mucho de la trama antes presentada.

El tema ha trascendido a tal punto que Brasil llevó un enérgico reclamo al 68.º periodo de sesiones de la Asamblea General de la [ONU](#).

Si bien, en los últimos meses numerosas han sido las denuncias de espionaje por parte de agencias del gobierno de los Estados Unidos, todas susceptibles de inspirar preocupación, definitivamente sí tenemos que preocuparnos acerca de la posibilidad de que dichas instancias cuenten con la habilidad y disposición de vulnerar los estándares actuales de cifrado y protección de información en Internet que, en caso de confirmarse su existencia, constituyen una grave amenaza a la esencia tecnológica de Internet y advertiría entonces un 0% privacidad y 0% seguridad.

Este tipo de iniciativas gubernamentales, sumadas a las recientes revelaciones sobre prácticas de vigilancia (caso de [Eduard Snowden](#), exinformático de la CIA), aún produciéndose fuera de la región, supondría un impacto sobre la privacidad y seguridad con la entidad, suficiente como para poner en peligro la interoperabilidad global de la Internet así como la capacidad que tiene esta de continuar siendo el motor de desarrollo que los países de América Latina y el Caribe necesitan.

El ciberespacio no tiene fronteras. La Web 2.0, la transparencia y la rendición facultada por una búsqueda en [Google](#), un video de [YouTube](#), o un [tweet](#), son amenazas directas a sistemas políticos restrictivos; la *World Wide Web* se convierte entonces en amenaza interna del régimen, de ahí el 100% de vigilancia electrónica para "preservar la seguridad nacional". Después de todo, Rusia, China, Irán y muchas otras naciones han impuesto fuertes filtros de Internet y sistemas de vigilancia.

Para empeorar las cosas, en los últimos meses, los Estados Unidos y el Reino Unido han puesto de manifiesto que han utilizado sus servicios de espionaje no solo en supuestos enemigos, sino también en las naciones amigas. Se refleja entonces una fobia que va a desestabilizar la visión de una Internet abierta, estable y segura.

Por otro lado, se ha argumentado que los estándares de seguridad brindan confianza a los usuarios de la red y si llegara a existir una mínima sospecha sobre la veracidad de estos, naturalmente la comunidad será más evasiva en aprovechar el máximo potencial que la red puede ofrecer. ¿Será que ahora vamos a vivir una "recesión" en la red? ¿Nos desconectaremos de EE. UU.? ¿Plantearemos nuestra propia infraestructura de Internet? ¿Tendremos una Internet dividida? Para Costa Rica, claro está, seguiremos mucho tiempo bajo la sombra del espionaje electrónico. Desde [Wikileaks](#) hasta Snowden, definitivamente han activado una alarma que ha puesto a correr a más de un diplomático y un técnico informático.

(*) *Académico Sede Regional Chorotega*