Este artículo es una publicación de la Corporación Viva la Ciudadanía
Opiniones sobre este artículo escribanos a:
semanariovirtual@viva.org.co
www.viva.org.co

2 años del caso Snowden: gobiernos insisten en ampliar vigilancia masiva

Cristina Fontenele
Estudiante de Periodismo en Faculdades Cearenses (FAC), publicista y Experta en Gestión de Marketing – Tomado de Adital

El informe “Dos años después de Snowden: protegiendo derechos humanos en una época de vigilancia en masa”, de Amnistía Internacional, advierte sobre la intención de los gobiernos de ampliar aún más la vigilancia masiva, a pesar de que la práctica es considerada una violación a los derechos humanos. El caso Snowden llamó la atención de la comunidad internacional y provocó tensión en la relación entre algunos países.

El 5 de junio de 2013, Edward Snowden, ex agente de la NSA (Agencia Nacional de Seguridad de Estados Unidos), reveló que los servicios de inteligencia de los países colaboraban entre sí para espiar e-mails, búsquedas en Internet y llamadas telefónicas, entre otras informaciones. El diario británico The Guardian publicó una serie de revelaciones sobre el fuerte esquema de espionaje del Gobierno de Estados Unidos y del Reino Unido en varios países del mundo.

Snowden afirma en el informe de Amnistía que: “si no encontramos la manera de controlar esta situación, un día descubriremos que las sociedades libres y liberales han dejado de existir”.

Según Sherif Elsayed-Ali, director adjunto de Asuntos Globales de Amnistía Internacional, sostuvo que “aunque la aprobación de la Ley de Libertad de Estados Unidos muestra que es posible reducir la vigilancia, las perspectivas de aprobación de poderes de espionaje aún más invasivos en Francia y Reino Unido pone de manifiesto que el ansia de los gobiernos por obtener cada vez más información sobre nuestra vida privada es insaciable”.

Con las revelaciones de Snowden, el mundo entero supo que empresas como Facebook, Google y Microsoft proveen informaciones sobre sus clientes a la NSA; también fueron grabados y analizados por la NSA mensajes de texto y llamadas telefónicas realizadas a México, Kenia y Filipinas.

Plan de protección a los derechos humanos en la era digital

Amnistía Internacional y Privacy International presentaron el pasado 7 de junio un plan de siete puntos en el que instan a los gobiernos a equilibraren el uso de

la vigilancia, incluyendo el adecuado control judicial y supervisión parlamentaria.

Según los grupos de derechos humanos, la vigilancia de las comunicaciones debe conservar los límites del derecho internacional, y ser aplicada solamente cuando el blanco de la vigilancia se configure con elementos de prueba suficientes de delito, y con autorización de una entidad estrictamente independiente como un juez, cuando sea supervisada por procesos parlamentarios y judiciales transparentes e independientes, y cuando esté regida por reglas y políticas disponibles públicamente y detalladas de manera suficiente.

Seguridad digital

Para ayudar a proteger su privacidad y hacer que sus llamadas telefónicas, *e-mails*, textos y *chats* sean más seguros, el sitio*web* de Amnistía Internacional, sugiere seis herramientas:

1. TextSecure – para mensajes de texto: Aplicación gratuita para Android (IPhone tiene una aplicación compatible con llamada Signal) que cifra sus textos, imágenes y archivos de video y audio.

2. Redphone – para llamadas de voz: Aplicación gratuita de código abierto para Android (para IPhone es la misma aplicación antes mencionada, Signal, que combina llamadas de voz y mensajes), que criptógrafa sus llamadas de voz de extremo a extremo.

3. Meet.jit.si – para llamadas de video y mensaje instantánea: Servicio gratuito de código abierto que protege sus llamadas de video, videoconferencias, mensajes instantáneos y transferencia de archivos. Existe también una versión para oficina llamada Jitsi, que puede bajarse para Windows, Linux, Mac LOS X y Android.

4. MiniLock – para intercambio de archivos: Este *plugin*, gratuito y de código abierto para su navegador *web*, permite criptografar y compartir archivos, incluyendo archivos de video, adjuntos de correo electrónico y fotos.

5. Mailvelope – para un correo electrónico más seguro: Complemento gratuito para el navegador, proporciona una criptografía extremo a extremo para correos electrónicos. Puede ser configurado para que funcione con casi cualquier proveedor de *e-mail* basado en la web, incluyendo Gmail, Yahoo y Outlook. Es de código abierto y utiliza criptografía OpenPGP.

6. SpiderOak – para intercambio y almacenamiento en la nube: Mantiene una copia de seguridad de sus archivos, sincroniza múltiples dispositivos y comparte archivos de manera privada con personas de confianza. Hace una criptografía completa de extremo a extremo de sus datos, lo que significa que, a diferencia de otros servicios de intercambio y almacenamiento en la nube, como Dropbox, ni siquiera la propia empresa puede ver sus documentos en sus servidores.

Edición 450 – Semana del 12 al 18 de junio de 2015