Internet, espionaje y extraterritorialidad

Desde 1960, Estados Unidos viene realizando actividades ilegales en las comunicaciones mundiales y las grandes telecos también espían

Juan Alfonso Fernández González / La pupila insomne

Las recientes revelaciones sobre el programa PRISM de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos, y la operación Tempora de la Dirección de Comunicaciones del Gobierno (GCHQ) del Reino Unido para realizar espionaje a las comunicaciones internacionales con la colaboración de las empresas que brindan los servicios más populares de Internet han sido recibidas con preocupación por millones de personas en todo el mundo que utilizan estos servicios.

Sin embargo, para muchos esta noticia no es más que una confirmación de algo ya ampliamente conocido, por lo que su importancia no radica en su novedad sino en que ha traído a la luz pública el debate sobre el endeble marco legal en el que se basa la operación y los servicios de Internet.

Pero antes de adentrarnos en las posibles consecuencias de estas revelaciones comencemos repasando lo que ya es sabido:

El Gobierno de los EE.UU. espía las comunicaciones mundiales

En 1960 fueron develadas por primera vez las actividades de espionaje a las comunicaciones mundiales que realizaba la Agencia de Seguridad Nacional (NSA), creada 8 años antes mediante una orden ejecutiva secreta del Presidente de los Estados Unidos.

Posteriormente, en 1977, surgió la red global de espionaje ECHELON operada por la NSA de conjunto con entidades de otros 4 países angloparlantes: Canadá, Reino Unido, Australia y Nueva Zelanda.

Este sistema cuenta con estaciones de intercepción electrónica y una flota de satélites para capturar, a escala mundial, todas las señales de comunicaciones que se transmitan por cualquier vía: por radio, satélite, microondas, red de telefonía celular, líneas telefónicas y fibras ópticas.

En el año 2001 el Parlamento Europeo “descubrió” la existencia de este sistema y expresó preocupación por su alcance, no sólo con relación a la intromisión en la vida privada de las personas, sino también por su uso con fines de espionaje industrial para brindarle una ventaja competitiva a las empresas de Estados Unidos con respecto a sus rivales europeas.

En el año 2003 se reveló una operación de espionaje a miembros del Consejo de Seguridad de las Naciones Unidas que se encontraban en esos momentos debatiendo la legitimidad de la invasión a Iraq. Esta operación, conducida por la NSA de los Estados Unidos contó con la participación de la GCHQ del Reino Unido.

Y desde hace 5 años la GCHQ ha venido desarrollando su propio programa, que en la actualidad intercepta más de 200 cables de fibra óptica que tocan tierra en las islas británicas, de donde extrae y procesa cada día 600 millones de llamadas telefónicas, todo esto realizado bajo acuerdos secretos con empresas comerciales a las que denominan “socios de intercepción”.

Las grandes empresas de telecomunicaciones e Internet espían a sus usuarios

Estas empresas almacenan los llamados “metadatos” de todo aquel que utilice sus servicios.

Se denomina metadato a aquella información sobre el “dato” y no al “dato” en sí. Por ejemplo, el contenido de una llamada telefónica o de un correo electrónico es el dato, mientras que los números telefónicos o direcciones electrónicas de su origen y destino, su localización física, la cantidad de segundos de la llamada o de palabras del e-mail, etc. son los “metadatos”.

Los metadatos permiten conformar los patrones del comportamiento de los usuarios de estas empresas, por lo que se tornan en un conocimiento valioso que es vendido a terceros que lo utilizan para colocar publicidad comercial, realizar análisis de mercados y otros usos.

De hecho los metadatos son el activo más importante de muchas grandes empresas de Internet, como Google, Yahoo y Facebook, entre otras, que obtienen de la venta de éstos la mayor parte de sus ingresos.

En ese sentido se ha señalado que la base de datos que posee Facebook con los perfiles de sus usuarios tenía hace un año un valor de mercado de más de 100 mil millones de USD. Por otro lado, se estima que la venta de este tipo de datos alcanzó en el 2012 los 6 mil millones de USD.

Esto es lo que les permite a estas grandes empresas de Internet ofrecer sus servicios de forma “gratuita” a sus usuarios, los cuales deben ceder su privacidad y consentir con que se recopile información sobre su persona.

Esta pauta generalizada abre una serie de interrogantes. Por ejemplo: ¿Tiene el mismo valor los metadatos de un internauta habitual de un país desarrollado que los de un ciudadano de un país subdesarrollado que ocasionalmente visita a Internet? ¿Será ese el motivo por lo que las inversiones para brindar los servicios de Internet tienen en cuenta a los consumidores y no a los ciudadanos? Estas preguntas definitivamente requieren un análisis que va más allá del contenido del presente artículo.

Finalmente: ¿Alguien puede asegurar que los “datos” de los usuarios no son también almacenados por estas empresas?

Racionalizando el espionaje

El gobierno de Obama ya había aprovechado la existencia de estas bases de datos empleándolas durante la campaña electoral del 2008. Por ello no debe extrañar que también se aprovechen para otros propósitos, entre ellos el espionaje.

Ello permite al Gobierno Federal lograr sustanciales ahorros ya que la adquisición de la información y su procesamiento inicial es realizada por estas empresas privadas lo que evita que la NSA tenga que realizarlo a partir de fuentes primarias como las de ECHELON.

En efecto, una de las diapositivas divulgadas sobre el programa PRISM lo caracteriza colectando la información directamente de los servidores de los proveedores de servicios y lo contrasta con otros sistemas que denomina “río arriba” (“Upstream”) que colectan las comunicaciones a medida que fluyen por los cables de fibras ópticas y otras infraestructuras.

Inmediatamente que se reveló el programa PRISM, las empresas involucradas en el mismo no les quedó más remedio que reconocer que habían entregado información de sus usuarios al gobierno federal, y aclararon que lo hicieron “en el marco de la ley”.

“Legalidad” del programa Prism y de la operación Tempora

La “ley” a que hacían referencia las empresas estadounidenses y bajo la cual deben entregar la información al gobierno federal es la llamada ley FISA (Foreign Intelligence Surveillance Amendment Act) que fue introducida por el Congreso de los Estados Unidos de América en el año 2008.

Esta ley fue redactada como reacción a las denuncias sobre las intercepciones sin orden judicial que se realizaron a ciudadanos norteamericanos como parte de un programa que instauró la administración de George W. Bush después del ataque a las torres gemelas.

La ley FISA no sólo dio una cobertura legal retroactiva a las intercepciones ya realizadas, sino que ratificó que el requisito de la orden judicial para acceder a los datos con fines de inteligencia sólo se aplica cuando éstos pertenecen a

ciudadanos de EE.UU.

Esto abrió las puertas a un espionaje masivo a los ciudadanos extranjeros que tengan sus datos en una empresa bajo la jurisdicción de los EE.UU.

En el caso de la operación Tempora de la GCHQ del Reino Unido, autoridades de ese país han señalado que la misma cumple “en su totalidad” con las leyes vigentes, en este caso las leyes RIPA (Regulation of Investigatory Powers Act), HRA (Human Rights Act) y la ISA (Intelligence Services Act).

Sin embargo se ha señalado que estas leyes, las cuales fueron redactadas en el siglo pasado, no se adaptan a la dinámica de la intercepción masiva de las comunicaciones contemporáneas, por lo que la aplicación de salvaguardas, como el requisito de una orden judicial para cada intercepción, ha sido flexibilizada, permitiendo la existencia de “certificados” los cuales “legalizan” la captura al por mayor de los datos procedentes del tráfico desde y hacia el exterior del Reino Unido.

Extraterritorialidad en la aplicación de estas leyes

La extraterritorialidad de la aplicación de estas leyes ha producido irritación en varios países aliados de los Estados Unidos y del Reino Unido.

Por ejemplo, en Australia se ha suscitado un debate sobre la “soberanía” de los datos que pertenecen a los australianos, tanto a las empresas como a las personas.

También la Canciller de Alemania, Angela Merkel expresó una (tibia) protesta en presencia del propio Presidente de los EE.UU. Barack Obama.

Pero el rechazo que posiblemente tenga repercusiones concretas es el expresado por la Unión Europea a través de Viviane Reding, su Comisionada de Justicia.

La Unión Europea se encuentra enfrascada en el proceso final de aprobación de una ley de protección de datos, la cual, en una versión que fue filtrada a la prensa en noviembre pasado, contenía un artículo, el número 42, especialmente redactado para contrarrestar los efectos extraterritoriales de la ley FISA de los EE.UU.

A partir de ese momento el Gobierno de los EE.UU. desplegó una campaña de presiones y “cabildeos” para persuadir a la Comisión Europea que “en aras de la guerra al terrorismo” no interfiriera en su capacidad de obtener inteligencia.

Aparentemente las presiones dieron resultado, pues la versión final de la propuesta de ley de protección de datos que fue presentada el pasado mes de enero no contenía el susodicho artículo. [15]

Sin embargo, a raíz de las revelaciones del programa PRISM, la Comisionada ha declarado que no tendría objeción alguna a la reintroducción del artículo al texto de la ley.

Internet debe ser regida por el derecho internacional

Toda esta extraterritorialidad en la aplicación de las leyes de los EE.UU. con respecto al acceso a los datos ha llevado a que en un editorial del periódico inglés The Independent se abogue por el establecimiento de reglas globales para la utilización de los datos que regule la actuación de las empresas trasnacionales de Internet.

Esto, unido a la necesidad de regular la gestión de los recursos críticos de internet, tal como fue explicado en un artículo anterior, y a los temas relacionados con la ciberguerra y la seguridad en internet, -que serán abordados en un próximo artículo- refuerzan la idea que Internet debe ser regida por el derecho internacional.

Por tanto, se deberá dar un impulso al debate sobre la gobernanza de Internet y considerar la posibilidad de avanzar hacia la negociación de un tratado que regule estos temas, así como otros aspectos de políticas públicas internacionales vinculadas con internet.

Ello ha ocurrido en otros ámbitos transfronterizos como la aviación civil, que desde el año 1947 es regida por la Convención de Chicago, o como el mar, que desde 1994 tiene la Convención de las Naciones Unidas sobre el Derecho del

Mar.

Internet se encuentra en una encrucijada

Puede seguir como hasta ahora, sin estar debidamente regulada, como una especie de “lejano oeste digital” donde se impone la ley del más fuerte y reine la desconfianza, lo que constituye un freno para el despliegue de más y mejores servicios, afectando negativamente no solo a los ciudadanos, sino también a las empresas.

O por el otro lado, Internet puede convertirse en un ámbito con un adecuado marco regulatorio, basado en los principios humanistas acordados durante la Cumbre Mundial sobre la Sociedad de la Información, lo que permitirá convertirla finalmente en un factor decisivo para el desarrollo económico y social y el logro de un mejor nivel de vida para todos.

Cuando ello ocurra Internet habrá llegado a su mayoría de edad.

* Juan Alfonso Fernández González es Asesor en el Ministerio de Comunicaciones y Profesor Adjunto en la Universidad de las Ciencias Informáticas de Cuba. Fue miembro del Grupo de Trabajo sobre Gobernanza de Internet de las Naciones Unidas y participó activamente en el proceso negociador de los documentos finales de ambas fases de la Cumbre Mundial sobre la Sociedad de la Información.