VIGILANCIA EN LA RED

O. Andrea Mendoza Enríquez.

Doctoranda por la Facultad de Derecho y Ciencias Sociales de la Benemérita Universidad Autónoma de Puebla. Becaria del Consejo Nacional de Ciencia y Tecnología. Profesora Investigadora del Fondo de Información y Documentación para la Industria INFOTEC.

Palabras clave: Libertad de expresión, seguridad nacional, Internet, mecanismos de control, soberanía, terrorismo.

La vigilancia en la red es un tema de actual relevancia para los Estados, ya que en mayor medida son éstos, los que llevan a cabo dicha práctica, como parte de sus estrategias en materia de seguridad nacional.

Esta práctica generalmente contraviene algunos de los derechos humanos de los usuarios de Internet, particularmente el relativo a la libertad de expresión, y vulnera la soberanía de las naciones, lo que ha ocasionado rupturas diplomáticas entre las mismas.

La vigilancia en Internet, consiste en un monitoreo permanente de los flujos de información, con la finalidad de detectar contenidos específicos en línea, lo que impacta en la arquitectura original de la Red, y conlleva a diversas formas de censura en Internet.

El aumento de las solicitudes oficiales de información formuladas por los Estados a los Prestadores de Servicios de Internet, propicia un particular interés en llevar a cabo estudios rigurosos del marco jurídico bajo el cual se materializa esta práctica; asimismo, provoca que se traiga a discusión, temas relacionados con los límites de la actividad del Estado y los derechos humanos en Internet, mismos que serán abordados en el desarrollo de este trabajo.

INTRODUCCIÓN

Las tecnologías de la información y comunicación han traído innumerables beneficios a la humanidad; sin embargo también han servido para llevar a cabo acciones que atentan en contra de la misma, particularmente en el rubro de los derechos humanos.

En el caso particular de Internet, se ha convertido en el medio más emblemático que ha roto paradigmas en la comunicación de las personas, pero al mismo tiempo, se ha vuelto motivo de disputa entre las naciones, particularmente en rubros de vigilancia de contenidos que fluyen a través de la Red.

La vigilancia en Internet se lleva a cabo por parte de un equipo de profesionales[1] dedicados a monitorear, predecir e interpretar las posibles acciones en el mundo virtual y en el real; sin embargo, tenemos que partir de la premisa de que la vigilancia tradicional no ha desaparecido del todo y muchas veces se complementan una a la otra: la policía continúa vigilando los cibercafés de Eritrea[2], todavía hay agentes vestidos de civil que persiguen a disidentes vietnamitas, y la intervención de los teléfonos de periodistas que facilitan el trabajo a los servicios de información**.** [3]

En la actualidad, las posibilidades que ofrece la vigilancia en Internet, amplía mucho el campo de acción de los gobiernos, por lo que representa un peligro para los derechos humanos.

En este sentido, *Wikileaks* en 2011 publicó los *spyfiles*[4] que mostraban la magnitud del mercado de la vigilancia en Internet y el mercado financiero que representa (más de cinco

---

[1] De acuerdo al libro *Numerati* de Stephen Baker, son ingenieros, matemáticos, o informáticos, que están cifrando toda la información que se produce en casi todas las situaciones. Los *numerati* estudian las páginas web de los usuarios de Internet, los alimentos que compra un consumidor, los teléfonos celulares, etc. Para ellos, los registros digitales crean un enorme y complejo laboratorio del comportamiento humano.

[2] El Estado de Eritrea es un país situado al noreste de África. Limita al norte y al oeste con Sudán; al sur con Etiopía y Yibuti; el este del país posee una extensa costa con el mar Rojo. Se independizó en 1993, lo que lo convierte en uno de los estados más jóvenes del mundo. Su capital y ciudad más poblada es Asmara. Eritrea es normalmente considerado como la Corea del Norte de África debido a que es un país "cerrado" como este último, entre otras similitudes.

[3] Consultado el 23/08/2013 en: http://orhpositivo.wordpress.com/2009/11/22/los-numerati-la-vigilancia-de-la-humanidad-a-traves-de-internet-desenmascarada/

[4] *The Spyfiles* es una recopilación de archivos sobre empresas de espionaje que ha hecho pública Wikileaks, y de acuerdo a Julian Assange, esas compañías en algunas ocasiones venden tecnología a regímenes opresores, con la finalidad de supervisar la actividad de los ciudadanos en la Red.

millones de dólares), así como la sofisticación de los productos que maneja"[5] temas que se desarrollarán en las siguientes líneas.

ANTECEDENTES

La seguridad nacional de los Estados ha sido la principal justificación para que los Estados intervengan directamente en la vigilancia de las comunicaciones de las personas, particularmente en Internet.

Los ataques de las torres gemelas del año 2001[6] establecieron el precedente de la vigilancia masiva de los Estados en Internet, así como de la colaboración entre los mismos, con la finalidad de evitar ataques terroristas.

A partir de este momento se impulsaron diversos proyectos relacionados a la instrumentación jurídica de la vigilancia en Internet, sin que hayan prosperado de inmediato, lo cual no significó que en la práctica no se materializara dicha vigilancia.

A manera de antecedente, en 1994, el presidente Bill Clinton firmó una ley que obliga a las compañías de telecomunicaciones a modificar sus equipos para permitir la vigilancia de redes de telefonía digital.

En 2001 George W. Bush autorizó a la *National Security Agency*[7] (NASA) para llevar a cabo varias formas de vigilancia electrónica dentro de Estados Unidos, incluida la de llamadas entre estadounidenses y posibles sospechosos de terrorismo.

En 2005, el gobierno de Bush exigió a las empresas de telecomunicaciones entregar los registros de llamadas de los clientes.

---

[5] Consultado el 13/08/2013 en: http://surveillance.rsf.org/es/

[6] Los ataques del 11-S marcaron el inicio de una operación sin precedentes por parte de la Agencia de Seguridad Nacional de los Estados Unidos de Norteamérica, que se había previamente concentrado en escuchas y desciframiento de contraseñas de extranjeros.

[7] La NSA rastrea en los registros usando algoritmos para detectar patrones que podrían dar señales de complots de posibles sospechosos de terrorismo.

El procedimiento radica en que las autoridades deben solicitar una autorización para la operación de vigilancia cada tres meses a la Corte de Vigilancia de Inteligencia Extranjera (un tribunal que funciona a puerta cerrada). Las autorizaciones permiten una búsqueda a través de registros de teléfono de metadatos[8], incluyendo la duración de las llamadas y la hora de realización, pero no el contenido de las conversaciones.

Por otro lado se encuentra la *Patriot Act*,[9] adoptada después del 11 de septiembre de 2001, y autoriza a la *Federal Bureau of Investigation* (FBI) a enviar cartas a Prestadores de Servicios de Internet para obtener las informaciones necesarias para vigilar sus cuentas, todo bajo la protección de no tener que revelar que estas demandas han sido realizadas.[10]

En 2008 el Congreso aprobó una enmienda a la *Foreign Intelligence Surveillance Act* (FISA)[11] que protege a las empresas de telecomunicaciones de demandas civiles por cooperar con el aparato de inteligencia de Estados Unidos.

En el ámbito internacional, otro de los instrumentos jurídicos que nacen a la postre de los atentados del 11 de septiembre de 2001, es el Convenio sobre la Ciberdelincuencia[12] también conocido como de Budapest, el cual ha tenido una evolución lenta.

En este sentido, las disposiciones más extensas y controvertidas del citado documento, son las relativas a la investigación y el procedimiento, que para el caso que nos ocupa, es el

---

[8] De acuerdo al Instituto Nacional de Estadística y Geografía de México (INEGI), los metadatos son datos altamente estructurados que describen información, describen el contenido, la calidad, la condición y otras características de los datos.

[9] Esta Ley fue declarada anticonsitutcional por la Corte americana.

[10] Consultado el 30/08/2013 en: http://www.fahrenheitmagazine.com/mundo/vigilancia-de-internet-por-el-fbi-es-inconstitucional/

[11] Conocida también como la *Ley de Vigilancia de la Inteligencia Extranjera* es una ley de los Estados Unidos que establece los procedimientos para la vigilancia física y electrónica y la recopilación de información de inteligencia extranjera entre potencias extranjeras y agentes de potencias extranjeras (los cuales pueden incluir ciudadanos estadounidenses y residentes permanentes sospechosos de actividades de espionaje o terrorismo).

[12] *The Convention on Cybercrime* (ETS) 185 o Convenio sobre Cibercriminalidad de Budapest (traducción no oficial) o "Convención sobre Delitos Informáticos" o "Convenio sobre Ciberdelincuencia" es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la ciberdelincuencia. Fue adoptado por el Comité de Ministros del Consejo de Europa en su sesión N° 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

requerimiento a los Estados para recolectar datos de tráfico y de contenidos (artículos 16 a 21), con la finalidad de facilitar las investigaciones relacionadas a cibercrimen[13].

En el caso particular de México, el Consejo de Europa en 2012 instó a dicho país para ratificar este Convenio, con la finalidad de reforzar políticas, estrategias, legislación y medidas prácticas sobre cibercrimen y seguridad cibernética[14].

Por otro lado, la Organización de las Naciones Unidas presentó un informe de 148 páginas titulado "El uso de Internet para fines terroristas", el cual determina que los medios por los que Internet se utiliza con fines terroristas son: propaganda, financiación, capacitación, planificación, ejecución y ciberataques[15].

VIGILANCIA EN INTERNET

La vigilancia en Internet constituía una práctica no reconocida por los Estados, hasta la revelación del ex asesor de inteligencia de Estados Unidos de Norteamérica, Edward Snowden, respecto a que el gobierno de ese país podía espiar a casi cualquier persona a través de Internet, sin necesidad de obtener una orden de la Corte.

Esta información fue confirmada por el periódico británico *The Guardian*, revelando detalles sobre las actividades de la NASA[16], la cual sería capaz de realizar un seguimiento de las personas, a través de sus mensajes de correo electrónico, las páginas web que consultan, las redes sociales y los GPS.

---

[13] Revista Chilena de Derecho y Tecnología. Centro de Estudios en Derecho Informático. Universidad de Chile. Consultada el 20/08/2013 en: http://www.rchdt.uchile.cl/index.php/RCHDT/article/viewFile/24030/25629

[14] Nota consultada el 06/03/2013 en: http://www.eluniversal.com.mx/articulos/69466.html

[15] Documento elaborado por *United Nations Office on Drugs and Crime. The use of Internet for terrorist purpose*s, consultado el 27/08/2013 en: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[16] Este Organismo cuenta con 40 000 empleados y con un presupuesto que se sitúa en los 10 mil millones de dólares. Asimismo, opera el programa de conciencia informacional total mundial, lo que presupone una constante vigilancia en Internet.

De acuerdo a Edward Snowden, las autoridades estadounidenses se han basado en la cooperación de las empresas de telecomunicaciones en los Estados Unidos, particularmente de Verizon, que transmitió miles de datos al gobierno, lo que trae a discusión la pérdida del derecho a la privacidad, en nombre de la lucha contra el terrorismo.

Actualmente tanto la NSA y como el FBI, están accesando directamente a los servidores centrales de las nueve compañías estadounidenses de internet[17,] para permitir el monitoreo 24 horas de correos electrónicos, documentos, videos, mensajes de redes sociales y fotos en línea.

Esto es posible a través de PRISM[18], el programa secreto ha estado activo desde 2007. Otro de los programas de vigilancia, conocido como BLARNEY, selecciona dispositivos de firmas, paquetes de direcciones y otros datos técnicos de internet.

Por su parte, en 2005 la Comisión Federal de Comunicaciones de Estados Unidos de Norteamérica, amplió el ámbito de aplicación de la ley para cubrir la información en Internet, obligando así a las empresas de banda ancha a garantizar el VOIP (Protocolo de voz en Internet) para que llamadas telefónicas pudieran ser intervenidas por el gobierno.

El programa de vigilancia PRISM que rastrea en los servidores de firmas de internet probablemente se apoya en la sección 215 de la ley Patriota (Patriot Act)[19.]

En el caso particular de la NASA, presta sus servicios y su capacidad de tratamiento al FBI, ya que fue esta oficina quien obtuvo la orden de telecargar los datos de las telecomunicaciones de todos los clientes de Verizon. Es decir, la NSA ofrece su capacitación pero es el FBI que tiene el mandato de espiar a los ciudadanos[20].

---

[17] Las firmas son Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube y Apple.

[18] El 11 de septiembre de 2007 el programa PRISM, cuyo costo anual es de 20 millones de dólares, empezó a obtener datos de Microsoft, según documentos publicados por el periódico The Guardian. El 12 de marzo de 2008, PRISM empezó a recolectar información de Yahoo, el 4 de enero de 2009 de Google, el 3 de junio de ese año de Facebook y el 7 de diciembre también de ese año, de PalTalk.
[19]Consultado el 09/08/2013 en:http://noticias.terra.com/eeuu/las-actividades-de-vigilancia-de-eeuu-desde-el-11-s,d9cb198de4e1f310VgnCLD2000000ec6eb0aRCRD.html

[20] Página *Radio Canada International*, Vigilancia de Estados Unidos en Internet: ¿qué implicaciones para los canadienses?, consultada el 13/08/2013 en: http://www.rcinet.ca/es/2013/08/09/vigilancia-de-estados-unidos-en-internet-que-implicaciones-para-los-canadienses/

Por otro lado, el informe sobre los Enemigos de Internet 2013, abordó la vigilancia en la red, determinándola como la actividad destinada a controlar las voces disidentes y la difusión de informaciones sensibles, llevada a cabo para prevenir toda desestabilización potencial del orden establecido.

En ese mismo año, el 12 de marzo Día Mundial Contra la Censura en Internet, se hizo pública una primera lista de cinco Estados enemigos de Internet[21.] Se trata de Siria, China, Irán, Bahréin y Vietnam.

Junto a los países, el Informe publicó además una lista de cinco empresas enemigas de Internet: *Gamma, Trovicor, Hacking Team, Amesys y Blue Coat.*

Estas empresas generalmente establecen vínculos comerciales con regímenes autoritarios, en los que sus productos se utilizan para vigilar a periodistas, disidentes e internautas.

Las encuestas realizadas por *Bloomberg, el Wall Street Journal y el Citizen Lab,* de la Universidad de Toronto, han revelado que las tecnologías para vigilar Internet utilizadas contra disidentes y activistas de derechos humanos, en países como Egipto, Bahréin o Libia provenían de empresas occidentales.

Algunas de estas tecnologías permiten además un doble uso: ser utilizadas con fines legítimos de lucha contra los delitos informáticos, o ser utilizadas como herramientas de vigilancia.

Organizaciones como Reporteros Sin Fronteras lleva tiempo exigiendo un control de la exportación de estas tecnologías a países que no respetan derechos fundamentales, lo que consideran un control que no debe quedar en manos exclusivas del sector privado, y que deben ser competencia de los legisladores.

Para el caso de la Unión Europea y Estados Unidos de Norteamérica, se ha prohibido la exportación de sistemas de vigilancia a Irán y Siria[22].

POSTURA DE LOS PRESTADORES DE SERVICIO

Los Prestadores de Servicio de Internet, como se ha dicho en líneas previas, han colaborados con los Estados, para facilitar la vigilancia en Internet; sin embargo, a últimas fechas, esta postura ha cambiado, en el sentido de pedir se modifiquen los protocolos de vigilancia en

[21] Son Estados que practican una vigilancia activa e intrusiva y que permite graves violaciones de la libertad de información y de los derechos humanos.

[22] Reporteros sin Fronteras. Enemigos de Internet. Informe 2013. Consultado el 30/08/2013 en: http://surveillance.rsf.org/es/

Internet, con la finalidad de informar a los usuarios respecto de los datos que se suministran y el tratamiento de los mismos.

Este cambio significativo de postura, se debe en gran medida al conflicto internacional que involucró a la NASA, derivado como ya se ha dicho, de las publicaciones de los diarios *The Guardian y The Washington Post*, que dejaron ver al mundo, la colaboración directa de los Prestadores de Servicio de Internet con diversos organismos oficiales, con la finalidad de acceder a sus datos, sin importar el derecho a la privacidad consagrado por instrumentos internacionales en materia de derechos humanos.

En este sentido, al menos 63 empresas de tecnología, inversores y grupos comerciales, solicitaron a través de una controversial carta al presidente de Estados Unidos de Norteamérica, Barack Obama, una mayor libertad para informar periódicamente sobre el número de peticiones que reciben del gobierno en sus programas de vigilancia.
Entre las empresas signantes, destacan *Apple, Google, Facebook y Microsoft, Dropbox, LinkedIn, Mozilla, salesforce.com, Tumblr, Twitter, Yahoo, Electronic Frontier Foundation, la Unión Americana de Libertades Civiles, el Centro para la Democracia y Tecnología, The Computer & Communications Industry Association, y la Fundación Wikimedia.*
La coalición también pidió que el gobierno, la emisión de un informe de transparencia con elementos básicos sobre cómo se utilizan los datos entregados.

A través de dicho documento solicitaron innovación respecto a la creación de mecanismos para garantizar que el gobierno sea transparente, responsable y respetuoso de las libertades civiles y los derechos humanos[23].

POSTURA DE LOS ESTADOS VIGILADOS

La comunidad internacional ha manifestado su desacuerdo con las prácticas de vigilancia practicadas particularmente por los Estados Unidos de Norteamérica; sin embargo, se debe

[23] Consultado el 14/08/2013 en: http://www.cubadebate.cu/noticias/2013/07/18/empresas-pediran-a-obama-mayor-transparencia-en-asuntos-de-espionaje/

destacar que al interior de muchos de estos países, se lleva a cabo este tipo de prácticas, con la finalidad de garantizar la seguridad nacional.

Derivado de lo anterior, viene a la luz el punto medular de la vigilancia en el contexto internacional, el cual radica en la soberanía de las naciones, o en su caso, en el reciente concepto de soberanía de los datos.

A continuación se detalla la postura de Brasil, México y Argentina respecto a la vigilancia en Internet llevada a cabo por los Estados Unidos de Norteamérica.

Brasil

De acuerdo a la presidenta de Brasil, Dilma Rousseff, su gobierno investiga la posible violación a su soberanía, derivado del espionaje de la NASA, particularmente respecto a llamadas telefónicas y correos electrónicos oficiales. La determinación radicará principalmente en comprobar si hubo participación de otros países o de otras empresas que no sean brasileñas.

Este país ha mostrado una postura de desacuerdo con este tipo de interferencias, que incluyen la vigilancia en Internet.

El tema es investigado por la Policía Federal Brasileña y por el ente regulador del sector de telecomunicaciones (ANATEL), que verificarán si empresas brasileñas de telecomunicaciones colaboraron con este tipo de espionaje de datos absolutamente privados de personas y de empresas privadas brasileñas.

Además, el gobierno brasileño revisará el marco de regulación de Internet, particularmente para obligar a que los datos de brasileños sean almacenados en Brasil.

Brasil solicitó una explicación al gobierno de Estados Unidos de Norteamérica y propondrá un debate sobre seguridad cibernética en el marco de la Unión Internacional de Telecomunicaciones (UIT) y en la Comisión de Derechos Humanos de las Naciones Unidas.

Este gobierno estableció una postura de privilegio de los principios fundamentales

consagrados en su Constitución, tales como la libertad de expresión y el derecho a la privacidad.[24]

México

A la luz de las revelaciones de vigilancia en Internet por parte de diversas agencias gubernamentales de los Estados Unidos de Norteamérica (NASA y FBI), se enfatizó la participación del gobierno de México en dicha práctica.

El gobierno de Felipe Calderón avaló en febrero de 2007 que el Departamento de Estado estadunidense instalara en México un sistema de intercepción de comunicaciones que permite la recepción, procesamiento, análisis y almacenamiento de llamadas telefónicas a escala nacional, así como de servicios de internet como chat, correo electrónico y voz sobre IP.

El contrato S-INLEC-06-R-4042[25] establece que la firma *Verint Systems* vendió equipo de espionaje al gobierno estadunidense con un valor de tres millones de dólares, el cual llegó a México a través de la Agencia Federal de Investigación (AFI) y la Procuraduría General de la República (PGR), con el fin de apoyar el combate al narcotráfico en el contexto de la Iniciativa Mérida[26].

El equipo usado por *Verint Systems* almacena hasta 25 mil horas y registra 60 llamadas simultáneas.

Ello implica que el gobierno estadunidense tiene acceso a la información que provea este sistema en México.

---

[24] Consultado el 15/08/2013 en: http://www.latercera.com/noticia/mundo/2013/07/678-532079-9-rousseff-asegura-que-brasil-investigara-violacion-de-soberania-en-caso-de.shtml

[25] Para mayor información, remítase a: http://e57355639224ae66447c-081e9ab4f283e1e4fe3c92bd954b97b4.r52.cf2.rackcdn.com/us-mx-spy.pdf

[26] Dentro de la justificación general de la Iniciativa Mérida para solicitar al gobierno federal de Estados Unidos 550 millones de dólares más para el año fiscal 2008, fechada el 23 de octubre de 2007, se menciona un gasto de 7.9 millones de dólares para "expandir la interconectividad de la base de datos de su Servicio de Inteligencia en México, y crear un sistema de operaciones para la seguridad en las redes de comunicaciones que permita administrar datos y contenga herramientas de análisis forense. Ese mismo año se firmó el contrato con Verint para la adquisición de lo que se conoce hoy como *Mexico Technical Surveillance System* (Sistema de Vigilancia Técnica México).

El citado documento señala que este sistema de intercepción de comunicaciones fortalecerá al gobierno de Estados Unidos y a la postura protectora de México en la difusión oportuna y precisa de información en cada país, desde el ámbito federal, estatal, local y privado.

Según se señala en el contrato, el equipo permite interceptar llamadas de destino de redes de Telmex, Telcel (TDMA y GSM), Nextel (iDEIM/GSM), Telefónica, Unefon, Iusacell (CDMA y TDMA), VoIP de Cisco Systems, paquete de datos de Prodigy, así como de otros prestadores de servicios de internet, y almacena hasta 25 mil horas. Tiene la capacidad de recoger, monitorear y registrar 60 llamadas simultáneas y mapearlas en segundos a nivel de calle, gracias al software MapInfo.

Una serie de contratos entregados a lo largo de 2012 y 2013 revelan detalles sobre la forma en que este sistema se ha convertido en parte clave en la lucha contra el narcotráfico y el terrorismo entre México y Estados Unidos.

Una actualización al contrato se dio el 27 de abril de 2012, la cual fue significativa en el trabajo de espionaje telefónico y de servicios de internet en México.

Según un documento del Departamento de Estado de Estados Unidos, en esa fecha se aumentó el número de estaciones de escucha, de 30 a 107, que fueron distribuidas en varias ubicaciones en el país, las cuales permiten ampliar el radio de captación de llamadas telefónicas.

Los legisladores del Congreso mexicano aprobaron por mayoría rechazar enérgicamente los actos de espionaje realizados por la Agencia de Seguridad Nacional de Estados Unidos.

Además, rechazaron categóricamente toda acción que vulnere la intimidad, la protección de datos personales o la seguridad de la población mexicana, o atente contra la soberanía que protege a las representaciones diplomáticas de México.[27]

Por su parte, el senado del mismo país solicitó a la Secretaría de Relaciones Exteriores un reporte sobre las acciones emprendidas por el Ejecutivo Federal, en relación al programa de vigilancia y espionaje internacional operado por agencias gubernamentales de Estados Unidos de Norteamérica.

[27] Consultado el 30/08/2013 en: http://www.excelsior.com.mx/nacional/2013/07/09/908167

Mediante boletín-1958 el Senado de México solicitó a la Secretaría de Gobernación sobre la estrategia en torno al monitoreo de información en el ciberespacio, con la finalidad de evitar vulnerar la privacidad de los usuarios y se salvaguarden los datos personales de los mismos.

Asimismo, se solicitó a la misma Secretaría explique el uso del software *Finfisher/Finspy* en las instancias de seguridad mexicanas.

Argentina

El caso de Argentina, no fue distinto al de Brasil, ya que mostró su inconformidad con las prácticas de espionaje por parte de los Estados Unidos de Norteamérica.

El gobierno argentino decidió unirse a Brasil para montar un blindaje informático contra el espionaje del país del norte.

Para tal efecto, los ministros de Defensa de ambos países Agustín Rossi y el brasileño Celso Amorim, respectivamente, emitieron una declaración de trabajo conjunto consistente en lograr una complementación en ciberdefensa, como uno de los puntos principales de la agenda bilateral en la materia[28].

POSTURA DE LAS ORGANIZACIONES CIVILES

Algunas organizaciones civiles pidieron al Congreso de los Estados Unidos de Norteamérica una investigación a fondo de la vigilancia en Internet, considerada como una violación a las libertades civiles y la privacidad.

En este sentido, la actual administración de Barack Obama enfrenta un proceso legal emprendido desde 2008 por un grupo de ciudadanos en contra del programa de intromisión.

[28] Consultado el 09/09/2013 en: http://www.jornada.unam.mx/ultimas/2013/09/13/222928441-argentina-y-brasil-pactan-impulsar-cooperacion-contra-espionaje-cibernetico

Las organizaciones civiles, particularmente la *Electronic Frontier Foundation* (EEF)[29], con sede en San Francisco California, consideran que la vigilancia en Internet, en específico la emprendida por el gobierno de los Estados Unidos de Norteamérica, no sólo afecta la confianza en el gobierno, sino también las formas en que los usuarios de Internet se comunican[30].

Por otro lado, la sociedad civil se ha dirigido una carta al Congreso de Estados Unidos de Norteamérica sobre la vigilancia en internet y telecomunicaciones

Miembros del Congreso de EE.UU.:

Escribimos como una coalición de organizaciones de la sociedad civil de todo el mundo para expresar nuestra seria alarma con relación a las revelaciones de vigilancia de las comunicaciones telefónicas y en internet de los ciudadanos de Estados Unidos y de otros países por el gobierno de los EE.UU. También deseamos expresar nuestra profunda preocupación de que las autoridades estadounidenses puedan haber puesto los datos resultantes de estas actividades de vigilancia a disposición de otros estados, entre ellos el Reino Unido, Holanda, Canadá, Bélgica, Australia y Nueva Zelanda. Muchas empresas de internet con sede en EE.UU. con alcance global también parecen estar participando en estas prácticas.

La introducción de mecanismos de vigilancia en el centro de las comunicaciones globales digitales amenaza gravemente a los derechos humanos en la era digital. Estas nuevas formas de poder descentralizado reflejan cambios fundamentales en la estructura de los sistemas de información en las sociedades modernas. Cualquier paso en este sentido debe ser examinado por medio de un amplio, profundo y transparente debate con toda la sociedad. La interferencia con los derechos humanos de los ciudadanos por parte de cualquier gobierno, propios o extranjeros, es inaceptable. La situación de un ciudadano incapaz de comunicar pensamientos privados y sin vigilancia por parte de un Estado extranjero no sólo viola los derechos a la intimidad y a la dignidad humana, sino que también pone en peligro los derechos

[29] Esta organización está dedicada, entre otras cosas, a defender las libertades en Internet.

[30] Obama y el Gran Hermano. Artículo consultado el 30/08/2013 en: http://www.proceso.com.mx/?p=344863

fundamentales a la libertad de pensamiento, opinión, expresión y asociación que se encuentran en el centro de toda práctica democrática. Este tipo de acciones son inaceptables y plantean serias preocupaciones sobre las violaciones extraterritoriales de los derechos humanos. La incapacidad de los ciudadanos para saber si son objeto de una vigilancia externa, para impugnar este tipo de vigilancia, o pedir reparación es aún más alarmante.

La contradicción entre la constante afirmación de los derechos humanos en línea por el gobierno de los EE.UU. y las recientes denuncias de lo que parece ser la vigilancia masiva de ciudadanos de Estados Unidos y de otros países por ese mismo gobierno es muy preocupante y conlleva repercusiones negativas en el escenario global. Una violación flagrante y sistemática de los derechos humanos articulados en los artículos 17 y 19 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), del cual Estados Unidos es signatario, así como los artículos 12 y 19 de la Declaración Universal de los Derechos Humanos debe de llamar nuestra atención. Teniendo en cuenta que los EE.UU. debe participar en una larga discusión, hace mucho, acerca de cómo actualizar y modernizar su política para alinearse con sus principios y documentos iniciales, lo que sucede a continuación en la supervisión legislativa y ejecutiva sucursal en los EE.UU. tendrá consecuencias enormes e irreversibles para la promoción y protección de los derechos humanos de las personas en todo el mundo.

También es notable que el gobierno de los Estados Unidos apoyó la Resolución de las Naciones Unidas Consejo de Derechos Humanos 20/8, que firma que los mismos derechos que la gente tenga fuera de línea también deben estar protegidos en línea, en particular la libertad de expresión… y hace apenas unos días, el 10 de junio, los EE.UU. fue parte de un grupo de países que redactó una declaración regional, que dice: que, al abordar los problemas de seguridad en Internet, esto debe hacerse de una manera consistente con las obligaciones del Estado en virtud del derecho internacional de los derechos humanos y el pleno respeto de los derechos humanos. Que al parecer no fue el caso de las últimas prácticas del gobierno de EE.UU. Además de representar una grave violación de los derechos humanos fundamentales de las personas en todo el mundo, la incoherencia entre las prácticas y las declaraciones públicas de los EE.UU. También socava la credibilidad moral del país dentro de la comunidad global que lucha por los derechos humanos, ya que se aplican

a Internet y afecta fatalmente la confianza de los consumidores en todas las empresas estadounidenses que prestan servicios en todo el mundo.

El pasado 10 de junio de 2013 muchos firmantes de esta carta se unieron para elevar nuestras preocupaciones al Consejo de Derechos Humanos de las Naciones Unidas. Lo hicimos en el contexto del reciente informe de la Relatora Especial de la ONU sobre el derecho a la Libertad de Opinión y Expresión, del Sr. Frank La Rue. Este informe apunta detalladas y preocupantes tendencias sobre la vigilancia de las comunicaciones por estados con graves consecuencias para el ejercicio de los derechos humanos a la vida privada y a la libertad de opinión y de expresión. Tomamos nota de que muchas personas y organizaciones estadounidenses ya habían escrito una carta al Congreso para expresar sus preocupaciones sobre las acciones de EE.UU. y la legalidad de éstas con relación al derecho interno.

También estamos muy decepcionados de que, en las declaraciones de las autoridades estadounidenses sólo han insistido en que no habían obtenido acceso al contenido relacionado a los ciudadanos de Estados Unidos, y que fue recogido sólo los metadados de sus comunicaciones. No ha habido una sola palabra sobre el tema de acceso a gran escala del contenido y datos relacionado con las comunicaciones de ciudadanos no estadounidenses, que constituye una casi segura violación de derechos humanos. El enfoque de las autoridades de Estados Unidos en la diferencia entre el tratamiento de los ciudadanos estadounidenses y no ciudadanos en un asunto que se refiere esencialmente a la violación de los derechos humanos es muy problemático. Los derechos humanos son universales, y todos los gobiernos deben abstenerse de violarlos para todas las personas, y no sólo para sus ciudadanos. Somos fervientes partidarios de que las disposiciones legales y prácticas actuales y futuras deben de tomar este hecho con la debida consideración.

Somos conscientes de que en la mayoría de los países, se obliga legalmente a las compañías de telecomunicaciones a preservar el tráfico de toda la información, no obstante queremos que se transparenten las normas y políticas mediante las cuales una autoridad competente ordena o permite el acceso a dichas comunicaciones, con el fin de tener la tranquilidad que no se está haciendo abuso de un mecanismo de control para privilegiar en unos casos el derecho de todos ante un derecho particular.

Por consiguiente, instamos al gobierno de Obama y el Congreso de los Estados Unidos a tomar medidas inmediatas para desmantelar las existentes, y evitar la creación futura de sistemas de vigilancia basados en telecomunicaciones y en Internet globales. Además, instamos al Gobierno de los EE.UU., el FBI y la Fiscalía General (Attorney General) para que las empresas implicadas o afectadas puedan publicar estadísticas de peticiones pasadas y futuras de la Ley de Vigilancia de Inteligencia Exterior (FISA) que han recibido o pueden recibir. Pedimos además al Congreso de EE.UU. que establezca protecciones para las fuentes gubernamentales de los periodistas con el fin de garantizar que el público esté informado adecuadamente acerca de los abusos de poder que violan los derechos humanos fundamentales de los ciudadanos de todos los países, EE.UU. y otros. También tomamos el pedido de la organizacion Humans Rights Watch para instar a la creación de un grupo independiente con poder de citación y de todas las autorizaciones de seguridad necesarias para examinar las prácticas actuales y formular recomendaciones para garantizar la protección adecuada de los derechos a la privacidad, la libertad de expresión y asociación. Los resultados de este panel deben ser publicados ampliamente[31].

CONSIDERACIONES FINALES

1. La seguridad nacional de los Estados es interés primordial en las políticas gubernamentales; sin embargo, esto no significa que con la finalidad de salvaguardar dicha seguridad, se transgredan derechos humanos de la mayoría de usuarios de Internet.
2. Si bien resulta necesario supervisar algunos flujos de información en Internet, se deben instrumentar los mecanismos que garanticen transparencia en el manejo de la información, y que salvaguarden en mayor medida los derechos de los usuarios de Internet.
3. La vulneración de la soberanía de los Estados, constituye un elemento grave en las relaciones diplomáticas y de paz común entre los países.
4. La sobrevigilancia en Internet vulneraría el principio de neutralidad de la red.

[31] Consultado el 12/08/2013 en: https://www.apc.org/es/news/carta-de-la-sociedad-civl-al-congreso-de-estados-u

5. Los instrumentos jurídicos internacionales que prevean vigilancia en Internet, no resultarán eficaces hasta en tanto no sean ratificados por todos los países.
6. El desarrollo indiscriminado de la vigilancia en Internet, constituye una forma de censura para sus usuarios.
7. La vigilancia en Internet se ha convertido en una de las luchas de poder entre distintos Estados, al ser uno de los objetivos el control de la información en la Red.