CRV-VIII-01-15

SERVICIOS DE INVESTIGACIÓN Y ANÁLISIS

DIRECCIÓN

CONGRESO REDIPAL VIRTUAL VIII

Red de Investigadores Parlamentarios en Línea
Marzo-agosto 2015

Ponencia presentada por

Korina Velázquez Ríos
(coordinadora)

"LOS DERECHOS FUNDAMENTALES DE LOS CIUDADANOS DE MÉXICO Y EL PROGRAMA DE VIGILANCIA DE LA AGENCIA NACIONAL DE SEGURIDAD (NSA) DE LOS ESTADOS UNIDOS"

Marzo 2015

Av. Congreso de la Unión Nº. 66, Colonia El Parque; Código Postal 15969,
México, DF. Teléfonos: 018001226272; (+52 ó 01) 55 50360000, Ext. 67032, 67034
e-mail: redipal@congreso.gob.mx

"LOS DERECHOS FUNDAMENTALES DE LOS CIUDADANOS DE MÉXICO Y EL PROGRAMA DE VIGILANCIA DE LA AGENCIA NACIONAL DE SEGURIDAD (NSA) DE LOS ESTADOS UNIDOS"

Korina Velázquez Ríos, Martha G. Cárdenas R., Alicia Esther González L., Viridiana López H., Anayanssin Méndez C., Violeta T. Miranda M., Víctor M. Torres P

"Las empresas dispuestas a colaborar con el gobierno y comprometer sus servicios y productos no merecen ser de confianza con sus datos. Porque si lo hacen para un gobierno, lo harán para otro" [1]

Edward Snowden

RESUMEN

Con el antecedente de las declaraciones de Edward Snowden en 2013, donde exhibió el trabajo de espionaje estadounidense a varios países, entre ellos algunos de la Unión Europea (UE); el Parlamento Europeo (PE) elaboró un informe en el cual se argumentan actos de vigilancia masiva, presentando una crítica a estas acciones, así como un balance sobre las competencias y facultades de la UE en materia de seguridad.

Las principales conclusiones del Parlamento Europeo en el Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad se enfocan en asignar recursos a países miembros para no depender tecnológicamente de otras naciones; lo que significaría disponer de servicios de almacenamiento *en nube* en territorio europeo, así como el desarrollo de software y paquete de protección de datos propios. Así mismo, emite recomendaciones para prohibir la vigilancia masiva generalizada en la UE por parte de Estados Unidos (EEUU); exhortando a los estados miembros a revisar sus legislaciones y prácticas nacionales en materia de servicios de inteligencia para evitar actividades de vigilancia que incumplan con las garantías jurídicas de la UE, así como promover un código de buenas prácticas que mejore el acceso de sus organismos de control a información sobre las actividades de inteligencia.

[1] Asociación de Internautas, Artículo "Hostil a la privacidad": Snowden insta a deshacerse de Dropbox, Facebook y Google" http://www.internautas.org/html/8568.html

I. Introducción

La violación a la privacidad de datos de los ciudadanos no solamente europeos, sino de varios países incluido México, se puso al descubierto en 2013 cuando Edward Snowden, ex trabajador de la NSA, hiciera públicas las prácticas de espionaje estadounidense a sus ciudadanos y a los gobierno de otras naciones. A partir de entonces, la Comunidad Europea así como otras naciones y la sociedad civil han levantado la voz para decir NO a estas acciones no controladas.

Para la UE, el uso de las nuevas tecnologías es una prioridad como lo apunta Lorenzo Cotino (2007. Pág. 113) al señalar que de acuerdo al "Plan de Acción eEuropa 2005", la Comisión Europea recomienda a sus Estado miembros, administraciones y gobiernos, el uso de las Tecnologías de la Información y la Comunicación (TIC) para acercar la Administración de un gobierno a su ciudadanía.

Ante esta recomendación ¿Cómo salvaguardar los datos personales? ¿Cómo asegurar que la información no tendrá otros usos? ¿Cómo garantizar los derechos fundamentales? ¿Cómo tener un control de los servicios de inteligencia?

Después de las declaraciones de Snowden, el Parlamento Europeo[2], bajo su jurisdicción como representante directo de los ciudadanos de la UE, realizó un informe sobre las prácticas de espionaje efectuadas por EU, analizando más de 50 documentos sobre garantías a los derechos fundamentales de los ciudadanos, como: los valores de respeto a la dignidad humana, la libertad, la democracia, la igualdad y el Estado de Derecho.

[2] El Parlamento Europeo se compone de 751 diputados elegidos en los 28 Estados miembros de la Unión Europea ampliada. Desde 1979, los diputados son elegidos por sufragio universal directo por un período de cinco años. http://www.europarl.europa.eu/aboutparliament/es/0081ddfaa4/Eurodiputados.html

II. Algunas consideraciones del Parlamento Europeo a la vigilancia masiva

Los programas de vigilancia masiva utilizados por algunos países, como Estados Unidos o Reino Unido, permiten acceder y rastrear todo tipo de información que revisa o genera un ciudadano cuando utiliza Internet.

De acuerdo al informe de la Alta Comisionada de la ONU para los Derechos Humanos[3], Navi Pillay "*la vigilancia masiva, así como la recolección y el almacenamiento de datos personales derivados de la comunicación digital -si forma parte de programas de vigilancia dirigida o masiva- no solo puede infringir el derecho a la privacidad, sino también un rango de otros derechos fundamentales*".

Este informe es importante ya que, además de que refuerza las ideas y conceptos sobre la vigilancia masiva, pone sobre la mesa la manera en que los estándares internacionales de derechos humanos sirven para evaluar prácticas que no están apegadas a la legalidad y el impacto producto del alcance y la masividad de Internet.

El Parlamento Europeo concluyó que la protección de datos y la intimidad son derechos fundamentales que el Estado debe garantizar, así como la seguridad para que la lucha contra el terrorismo se atienda en el marco del Estado de Derecho, y se cumpla la libertad de expresión y el secreto profesional como debió ocurrir en los casos de *The Guardian* o *Der Spiegel*, en los que se exhibió el alcance de los sistemas de vigilancia nacionales y extranjeros en países europeos.

En el contexto del respeto de los derechos fundamentales, las autoridades estadounidenses y europeas, deben prohibir la vigilancia masiva generalizada, los estados de la UE evaluar y revisar sus legislaciones y prácticas nacionales sobre los servicios de inteligencia y abstenerse de aceptar datos de terceros países recopilados ilegalmente; además de no permitir actividades de vigilancia ilegales en el marco de las garantías jurídicas de la UE, asumiendo la obligación de proteger a sus ciudadanos de la vigilancia ilegal, y exhortando a emprender acciones contra atentados a su soberanía y la violación del derecho internacional público.

Los principios de puerto seguro[4] han demostrado que no proporcionan una protección adecuada, por lo que los Estado miembros, deben suspender el flujo de datos

[3] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[4] El Acuerdo de "Puerto Seguro" consta de siete principios básicos, referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), transferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados). Dichos principios son, como se indicó,

a cualquier organización que haya autocertificado su adhesión a los principios de puerto seguro de EEUU (empresas como *Google*, *Facebook*, *Yahoo*, etc.); asimismo, se deben establecer cláusulas contractuales o normas empresariales vinculantes que establezcan garantías y protecciones específicas que protejan la intimidad, los derechos y libertades fundamentales. Por otro lado, la transferencia de datos puede ser suspendida cuando se impongan requisitos más allá de los principios de las sociedades democráticas y que tengan efecto negativo en sus garantías.

En el año 2000[5] los principales motores de búsqueda en la red comenzaron a asociarse, lanzando complementos en forma de aplicaciones, como "nuevos navegadores" y "barras"; las cuales recopilaban información de los usuarios durante toda la interacción en Internet.

Para 2003 con el éxito de los navegadores en constante desarrollo, se puso a disposición de los usuarios en Internet los servicios de búsquedas de productos, donde se perfeccionan sistemas como *Adsense* de *Google*, *Google Books*, y otros.

El *marketing* comenzó a ser el eje de los sitios a los que se tenía acceso de interacción y creación de forma "gratuita", la evolución llevó a las aplicaciones de geolocalización que para su uso requieren de información personal (números de teléfono, direcciones físicas, cuentas bancarias, etc.), con ello NSA[6] de los EEUU resolvía las encriptaciones de estas empresas, a las cuales en 2007 tenía atadas bajo el Programa de Vigilancia Electrónica "*PRISM*"[7] (y otros como *Xkeyscore*, *Echelon*, *Bullrun*), toda empresa que no colaborara con PRISM sería fuertemente multada. Rápidamente todos los servicios de *Google*, *Apple*, *Microsoft*, *Dropbox*, *Yahoo*!, *AOL*, *Skype*, *Youtube*, *Paltalk*, *Facebook*, etc., aceptaron.

III. Servicios de Inteligencia

De acuerdo con Wikipedia, un servicio de inteligencia[8] es una organización gubernamental privada, dedicada a obtener información para la seguridad nacional y la

---

complementados con las "preguntas más frecuentes", básicamente referidas a tipos específicos de datos o tratamientos.
http://www.agpd.es/portalwebAGPD/internacional/adecuacion/estados_unidos/common/pdfs/ElAcuerdodePuertoSeguroconlosEstadosUnidos.pdf

[5] Google Empresa. *Nuestra Historia en profundidad.* https://www.google.com/about/company/history/?hl=es#top

[6] Wikipedia, *Agencia de Seguridad Nacional* http://es.wikipedia.org/wiki/Agencia_de_Seguridad_Nacional

[7] Wikipedia, *PRISM* http://es.wikipedia.org/wiki/PRISM

[8] Wikipedia. Servicio de inteligencia. http://es.wikipedia.org/wiki/Servicio_de_inteligencia

defensa del país. Su propósito es, obtener información para contribuir a salvaguardar los intereses del Estado, su integridad y su seguridad territorial.

Para Fernando Velasco, director de la Cátedra Servicios de Inteligencia y Sistemas Democráticos de la Universidad Rey Juan Carlos "*la inteligencia como órgano preventivo por naturaleza aparece como uno de los principales instrumentos para anticiparse a las nuevas amenazas y afrontar el nuevo y cambiante escenario de seguridad*"… "*Estar bien informado no garantiza por sí mismo mejores decisiones, pero estar poco informado o desinformado reduce considerablemente las posibilidades de éxito*", agrega.[9]

En 2013[10][11] estalló la presión hacia las Agencias de Inteligencia, exigiendo transparencia y controles de publicación sobre las actividades que realizan, a fin de moderar el nivel de secretismo y garantizar la seguridad de los ciudadanos. Incluso los programas de gobierno de la UE proponen invertir en servicios de nube como fuente de crecimiento y empleo de este mercado bajo determinados filtros para vigilancia, seguridad informática, encriptación y desarrollo de aplicaciones.

El Parlamento Europeo propuso entonces la creación de un grupo de alto nivel el que contara con estándares mínimos europeos por lo que se refiere al control de los servicios de inteligencia y recomendaciones existentes de organismos internacionales como las Naciones Unidas o el Consejo de Europa. Otra función de este grupo será la de desarrollar criterios para una mejor transparencia a partir del principio general de acceso a la información y de los llamados "Principios de *Tshwane*"[12] que son parámetros mundiales relativos a la seguridad nacional y el derecho a la información; éstos fueron desarrollados con objeto de orientar a quienes estén involucrados con la redacción, revisión o implementación de leyes y disposiciones relacionadas con la autoridad del Estado para ocultar información por motivos de seguridad o castigar la divulgación de la misma.

---

[9] Juan Paullier. El mundo del espionaje latinoamericano. BBC Mundo. http://www.bbc.co.uk/mundo/america_latina/2009/11/091118_espionaje_latinoamerica_jp.shtml

[10] Tendencias21. *Google, Facebook, Microsoft,… revelan sus cuentas con las agencias de inteligencia.* http://www.tendencias21.net/conocimiento/Google-Facebook-Microsoft-revelan-sus-cuentas-con-las-agencias-de-inteligencia_a34.html

[11] MedellinStyle.com. *La Agencia de Seguridad Nacional de EE.UU. tiene acceso a Google, Facebook y Sky.*

[12] Los Principios de *Tshwane* sobre Seguridad Nacional y Derecho a la Información fueron presentados en junio de 2013 por 22 organizaciones y centros académicos de todo el mundo. Los principios se desarrollaron con el fin de orientar a quienes estén involucrados en la redacción, la revisión o la implementación de leyes y disposiciones relacionadas con la autoridad del estado para ocultar información por motivos de seguridad o castigar la divulgación de la misma. Se fundamental en el derecho internacional, el derecho y los estándares regionales, la evolución de la práctica del estado, los principios generales del Derecho reconocidos por la comunidad internacional, y la producción escrita de expertos en la materia. http://www.right2info.org/exceptions-to-access/national-security

Asimismo, el Parlamento solicitó a los Estado miembros, que elaboraran un código de buenas prácticas para mejorar el acceso de sus organismos de control a la información sobre las actividades de inteligencia, e instó a la Comisión a que organizara una conferencia antes de diciembre del 2014 en la que participaran organismos nacionales de control y del marco jurídico, ya fueran parlamentarios o independientes, y se debatiera sobre los derechos humanos fundamentales, las normas sobre privacidad de datos aplicables de la UE, y la seguridad de las naciones.

Se invita a la Oficina Europea de Policía EUROPOL[13] a hacer pleno uso de su mandato para solicitar a los Estados integrantes de la UE que emprendieran investigaciones penales sobre ataques cibernéticos y delitos informáticos de gran calado con un posible impacto transfronterizo; considera que el mandato de la EUROPOL debería mejorar para estar en condiciones de iniciar su propia investigación derivado de la sospecha de un ataque contra los sistemas de redes e informáticos de los Estados miembros u organismo europeos.

Ante la vigilancia entre las naciones y de los Estados a sus gobernados algunos países que conforman la UE proponen la instauración de un recurso jurídico que "ampare" a la ciudadanía ante posibles arbitrariedades al derecho de sus libertades; es decir, se exhorta a las naciones a garantizar la seguridad a la privacidad, integridad e intimidad de las personas para evitar manejos inadecuados de datos, información, contenidos que empresas, gobiernos y particulares dispongan para efectos de chantaje, segregación, limitación o discriminación.

En ese sentido, el Parlamento recomienda se incorpore el "*Habeas corpus* digital europeo"[14] recurso legal reconocido para salvaguardar las libertades individuales frente a la acción arbitraria del Estado o empresas privadas, en virtud de que los datos personales que se encuentran en las redes digitales pueden revelar parte de la identidad, hábitos y preferencias.

Algunas acciones que recomienda el Parlamento Europeo son, entre otras, la suspensión del puerto seguro para la recopilación, uso y conservación de datos personales acordado entre EEUU – UE, así como del acuerdo TFTP[15] también con la misma nación relacionada al combate contra el terrorismo.

---

[13] www.europol.europa.eu

[14] Habeas Corpus Digital de la UE protegería la intimidad. http://www.eppgroup.eu/es/video/Un-H%C3%A1beas-Corpus-digital-de-la-UE-proteger%C3%ADa-la-intimidad

[15] En junio de 2010 la UE y EUA acordaron el flujo oficial de información sobre tratamiento y transferencia de datos financieros para el seguimiento de financiamiento al terrorismo. Cuyo propósito es acceder a datos

El informe en el apartado que se señala, exhorta a la Comisión Europea a analizar un marco legal que defina un programa europeo de protección a denunciantes[16] (apegándose al secreto profesional) ante cualquier delito que atente contra las naciones y personas; y que garantice la investigación de la denuncia expuesta y la protección internacional de la integridad del denunciante.

Finalmente, el Informe realizado por el Parlamento Europeo sobre el Programa de Vigilancia de la Agencia Nacional de Seguridad de los Estados Unidos, en la parte de anexos brinda la metodología empleada para la redacción del informe.

IV. Espionaje en México

La historia de espionaje en México se remonta desde hace ya varias décadas, Raymundo Riva Palacio[17], afirma que existió "*The Mexican War Spy Company*" ("Compañía de Espionaje de la Guerra Mexicana"), servicio de inteligencia ideado por EEUU durante la invasión a México en 1847-1848; y que, para la década de los 60´s y 70´s la inteligencia estadounidense en México operada por la Agencia Central de inteligencia (CIA, por sus siglas en inglés) dirigió operaciones clandestinas contra los países comunistas. Agrega que existe una colaboración de inteligencia institucional, legal, legítima y acordada entre EEUU y México. Sin embargo, habría que revisar, la forma cómo el gobierno mexicano le ha otorgado atribuciones a los servicios de inteligencia de Estados Unidos en los últimos años, por fuera de los acuerdos institucionales, y en algunos casos, al margen de la ley. En el gobierno de Felipe Calderón, la colaboración con Estados Unidos alcanzó máximos sin precedente a nivel institucional, como puede verse en el documento que firmaron ambas naciones[18].

Este convenio señala que el gobierno estadounidense tiene la capacidad para interceptar, analizar y usar la información de todos los sistemas de comunicaciones que operan en México. El sistema, se señala en dicho documento, ayudará a disuadir, prevenir y mitigar actos de importantes delitos federales en México que incluyen el narcotráfico y el terrorismo. Al respecto, existe información acerca de que el gobierno mexicano, al hacerse públicas las declaraciones de Snowden, revisó los contratos por

---

personales con la posibilidad de eliminarlos o bloquearlos. Siendo aplicable únicamente a ciudadanos con nacionalidad de uno de los estados miembros de la UE o que tengan residencia permanente en uno de ellos. http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/otros_derechos/TFTP-ides-idphp.php

[16] http://www.eurosocial-ii.eu/documents/10192/740630/DT_2_Sistemas_denuncias.pdf?version=1.0.

[17] Raymundo Riva Palacio. "Espionaje en México, una vieja historia". La Razón. Julio 13, 2013. Disponible en http://www.razon.com.mx/spip.php?page=columnista&id_article=180583

[18] http://cryptome.org/2012/06/us-mx-spy.pdf

medio de los cuales se adquirió equipo de intersección de comunicaciones para que pudieran ser usados por el gobierno estadounidense, a fin de intervenir llamadas y otro tipo de comunicaciones en nuestro país en el marco de un convenio firmado en la Iniciativa Mérida[19]. El entonces embajador de México en Estados Unidos, Eduardo Medina Mora, indicó que *el espionaje es una práctica que, de confirmarse, resulta inaceptable e ilegal e ilegítima*, pero se debe procurar *que no descarrile la relación, porque es demasiado importante para los mexicanos y los estadounidenses*.[20]

Por otra parte, *Privacy Internacional* publicó en 2013 un informe sobre el derecho a la privacidad[21] donde externó su preocupación por las prácticas de vigilancia en México. Señala que en 2012, la Secretaría de la Defensa Nacional compró *software* de vigilancia para ser utilizado por el ejército mexicano sin transparencia en la compra y sin dar a conocer para qué se usaría el software.

Citizen Lab[22] publicó en 2013 una investigación sobre un programa de *spyware* llamado "FinFisher" adquirido por gobiernos de muchos países. Asimismo, activistas internacionales denunciaron haber sido intervenidos con él.[23]

En junio de 2013, asociaciones civiles mexicanas, tales como ContingenteMX y Al Consumidor, presentaron una denuncia ante el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) para que investigaran el uso de FinFisher en sus servidores porque estaban en riesgo sus datos personales.[24]

---

[19] Iniciativa Mérida. http://spanish.mexico.usembassy.gov/es/temas-bilaterales/mexico-y-eu-de-un-vistazo/iniciativa-merida.html Cuyo objetivo era aumentar la seguridad y combatir al crimen organizado, ha servido como escaparate para la transferencia libre de información entre EU y México.

[20] DiarioJurídico.com.mx. "Sobre la mesa" presunto espionaje de EE. UU. A México. Noviembre 22, 2013. Disponible en http://diariojuridico.com.mx/actualidad/noticias/sobre-la-mesa-presunto-espionaje-de-ee-uu-a-mexico.html

[21] Vermer, A. (2013, July). Corruption scandal reveals use of FinFisher by Mexican authorities. *Privacy International*. http://www.privacyinternational.org/blog/corruption-scandal-reveals-use-of-finfisher-by-mexican-authorities.

[22] Privacy International (2013). *The Right to Privacy in Mexico, Stakeholder Report Universal Periodic Review 17th Session*. London: Privacy International. https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/mexico_stakeholder_report_-_privacy_international.pdf

[23] *Communications surveillance in the digital age. México: El Caso FinFisher.* Trad. Korina Velázquez. GISWatch, Washington D.C., 2014. http://www.giswatch.org/es/country/m-xico

[24] http://es.globalvoicesonline.org/2013/06/22/mexico-activistas-piden-investigacion-del-software-espia-finfisher/

La Sociedad Civil contra la vigilancia masiva

El pasado 11 de febrero de 2014 usuarios de Internet de todo el mundo rechazaron la vigilancia masiva cuando se llevó a cabo la campaña "*The Day We Fight Back*" (El día que nos defendamos). Así, organizaciones como *Human Rights Watch*, la sociedad civil, sitios web y empresas de todo el mundo se unieron para oponerse a esta práctica de espionaje.

A raíz de esa campaña, expertos en derechos humanos de todo el mundo, redactaron y publicaron los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*[25]. Estos principios, que han sido firmados por más de 350 organizaciones, constituyen un esfuerzo importante realizado por la sociedad civil global para proteger el derecho a la intimidad del ciudadano digital; y proporcionan un marco para evaluar si las leyes y prácticas de vigilancia, actuales o propuestas, están en línea con los derechos humanos.

Conclusiones útiles para México

Gobiernos como los de Estados Unidos y sus aliados, con su enorme poder económico y tecnológico, han sido descubiertos vigilando masivamente a los gobiernos de casi todo el mundo, incluyendo a los ciudadanos usuarios de Internet y las TIC.

Es así que un internauta es susceptible de otorgar sus datos personales y sus patrones de conducta a desconocidos "sin su consentimiento". Ya sea para fines de seguridad nacional y que, por falta de regulación, usados en forma discrecional incluso para fines personales de algún trabajador de gobierno corrupto, algún delincuente o en el mejor de los casos, sólo para algún provecho comercial en línea.

La denuncia de la vigilancia hecha por Edward Snowden, situó al mundo en una realidad diferente. Los elementos de la ciencia ficción, parecen ser realidad, un poder que todo lo domina, un ojo vigilante que todo lo ve, el *Big brother*, registrando comportamiento para denunciar, juzgar, perseguir, etiquetar, eliminando la presunción de la inocencia y pasando casi directamente a la sanción.

No se duda que existan individuos o grupos sociales que se organicen para realizar actividades ilegales u opositoras, lo que de ninguna manera justifica que por ello se violen sistemáticamente los derechos humanos para vigilar actividades privadas.

[25] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Mayo 10, 2014. https://es.necessaryandproportionate.org/text

¿Qué conclusiones se deben alcanzar dada la gravedad de una situación que es una clara amenaza para las naciones del mundo?

- Una primera conclusión útil para México es que los estándares internacionales de Derechos Humanos sirven para evaluar las prácticas que no están reguladas aun, sobre todo, ante el poder e impacto masivo que ofrecen los nuevos desarrollos tecnológicos.
- La experiencia internacional muestra que debe evitarse anteponer un derecho humano fundamental sobre otro. Por principio de proporcionalidad la seguridad, el derecho de privacidad y protección de datos personales, así como el de transparencia, acceso de información y libertad de expresión deben estar igualmente garantizados por el Estado.
- El Parlamento Europeo identifica como vulnerabilidad el que se tenga un alto grado de dependencia a la tecnológica desarrollada por Estados Unidos; que gran parte de la información se encuentre en servidores establecidos geográficamente en otro país o que los proveedores de los servicios sean de compañías estadounidenses, debido a que eso permite ser susceptibles a filtraciones de información.
- Asimismo, se concluye que a pesar de las adversidades se debe buscar una estrategia para lograr una gobernanza democrática de Internet e invertir fondos en investigación y desarrollo que permita independencia tecnológica, como medida de seguridad y protección de datos e información clasificada.
- En este análisis la conclusión obligada es que se deben poner barreras y prohibiciones explícitas a las prácticas de vigilancia masiva porque nadie tiene derecho a violar la privacidad, la libertad y el ejercicio libre de los derechos, llámese Estado, grupo o individuo.

Recomendaciones para México

- Incidir mediante la exposición pública del tema para que se exija al Estado poner atención a este tipo de conductas que amenazan los derechos fundamentales.
- Profundizar en el conocimiento de las investigaciones del Parlamento Europeo, de modo que en Latinoamérica se aprenda de la experiencia para hacer un “frente común” que defina una postura unánime y adopte medidas de seguridad para la región.

- A partir de los logros alcanzados por el Parlamento Europeo respecto de la protección de los derechos de sus ciudadanos ante las acciones de vigilancia del gobierno y las empresas estadounidenses, México debe exigir el mismo nivel de respeto y cumplimiento para sus ciudadanos.
- El Estado mexicano debe cumplir con su obligación plasmada en la *Carta Iberoamericana de Gobierno Electrónico* de "reconocer al ciudadano el derecho de relacionarse electrónicamente con el gobierno" a través de sus servicios en línea, sin que esto signifique que estará expuesto a una vigilancia masiva o selectiva por parte del gobierno mexicano o de cualquier otro. Lo anterior, tomando como marco de referencia la Ley de Telecomunicaciones que brinda la posibilidad del espionaje telefónico y utilización de servicios de geolocalización, sin necesidad de una orden judicial.
- Subsanar la desventaja ciudadana para salvaguardar los derechos fundamentales de los ciudadanos y la sociedad en general, a partir de la expedición de una normatividad que cumpla con estándares internacionales, que brinde recursos legales para que el ciudadano pueda protegerse ante posibles arbitrariedades por parte del Estado.
- Alentar capacidades y estudios en materia digital, para generar expertos que asesoren y recomienden medidas de prevención a los usuarios de las tecnologías de la información, así como de las actividades que constituyan posibles delitos.
- Se recomienda que el marco normativo en México en materia de protección de datos y privacidad haga obligatoria la "Evaluación de Impacto de Privacidad" o *Privacy Impact Assessment* (PIA conocida por sus siglas en inglés) en el diseño de políticas públicas para evitar riesgos en el tratamiento de datos personales y violaciones a derechos fundamentales de los ciudadanos.
- Actualizar el marco jurídico para establecer reglas transparentes en el uso de *software* de espionaje y otras herramientas similares por parte del gobierno mexicano. Así como promover una guía de buenas prácticas y sanciones que restrinja el acceso de actividades de inteligencia generalizado e injustificado; así como abstenerse de aceptar datos provenientes de terceros países que sean recopilados ilegalmente.

- México debe ratificar las *Directrices para la Regulación de los Archivos de Datos Personales Informatizados de la Organización de las Naciones Unidas* (ONU)[26] como un marco de protección de su privacidad y sus datos personales, así como de protección de las comunicaciones de los individuos y de la privacidad en Internet.
- Que México se apegue a las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, a las que se adhirió el 18 de mayo de 1994.
- Que el Poder Legislativo tome una participación activa en la discusión de los temas de vigilancia del gobierno, así como de protección a la privacidad de las comunicaciones. Para lo cual, se deberá crear una Comisión Especial que analice las revelaciones de Edward Snowden acerca de la vigilancia de la NSA a los mexicanos, casos de uso de *software* para vigilancia como el FinFisher, de seguimiento a las acciones del Parlamento Europeo en la materia con objeto de proponer una adecuación al marco jurídico que brinde certeza legal para el ejercicio de los derechos humanos.
- Exigir al gobierno mexicano que se asignen recursos para una política digital que incluya el desarrollo de servicios de almacenamiento propio en la nube, *software* de código abierto y demás herramientas que fomenten la autonomía de México en uso de herramientas tecnológicas y su presencia en Internet.
- Establecer campañas de difusión para que la sociedad civil esté consciente de la importancia de la privacidad y conozca los riesgos de la vigilancia.
- Finalmente, recomendar que la participación de los usuarios en las redes digitales, sea democrática, incluyente, que aliente su mejor uso y se remarque nuestros derechos fundamentales de actuar con libertad, aprovechando las TIC como herramientas de desarrollo económico y social.

[26] *Cfr. Directrices para la regulación de los archivos de datos personales informatizados.* ONU, 1990. http://inicio.ifai.org.mx/DocumentosdeInteres/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf

Fuentes

CASTELLS, Manuel (editor), *La Sociedad Red: una visión global*, Alianza Editorial, 2006.

COTINO Hueso Lorenzo. *Democracia, participación y voto a través de las nuevas tecnologías*. Granada. Comares. 2007

En Internet

58 -- Communications Intercept System Mexico Solicitation Number: Agency: U.S. Department of State. Office: Bureau of International Narcotics and Law Enforcement Affairs. Location: INL RM MS http://cryptome.org/2012/06/us-mx-spy.pdf Fecha de acceso 12 de octubre de 2014

Communications surveillance in the digital age. México: El Caso FinFisher. Trad. Korina Velázquez. GISWatch, Washington D.C., 2014. http://www.giswatch.org/es/country/m-xico Fecha de acceso 31 de enero de 2015

Centro Nacional de Inteligencia *¿Qué es un servicio de inteligencia?* http://www.cni.es/es/preguntasfrecuentes/pregunta_001.html?pageIndex=1&faq=si&size=15 Fecha de acceso 27 de octubre de 2014

Convenio del Consejo de Europa sobre protección de datos. http://www.coe.int/t/dghl/standardsetting/dataprotection/global_standard/D%C3%A9pliant%20Conv108_es.pdf Fecha de acceso 12 de octubre de 2014

Convenio Europeo de Derechos Humanos

http://www.echr.coe.int/Documents/Convention_SPA.pdf Fecha de acceso 12 de octubre de 2014

Decisión n° 520/2000 de la Comisión de 26 de julio de 2000

- http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf Fecha de acceso 12 de octubre de 2014

Diario Oficial de la Unión Europea. Fecha de acceso 12 de octubre de 2014

Diario Oficial de la Unión Europea. Versión Consolidada del Tratado de la Unión Europea (TUE) http://www.boe.es/doue/2010/083/Z00013-00046.pdf Fecha de acceso 12 de octubre de 2014

Diario Oficial de la Unión Europea. Versión Consolidada del Tratado de Funcionamiento la Unión Europea (TFUE) http://www.boe.es/doue/2010/083/Z00047-00199.pdf Fecha de acceso 12 de octubre de 2014

Directrices para la regulación de los archivos de datos personales informatizados. ONU, 1990. http://inicio.ifai.org.mx/DocumentosdeInteres/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf

El Acuerdo de Puerto Seguro con los Estados Unidos de América http://www.agpd.es/portalwebAGPD/internacional/adecuacion/estados_unidos/common/pdfs/ElAcuerdodePuertoSeguroconlosEstadosUnidos.pdf Fecha de acceso 24 de octubre de 2014

García González Aristeo. La protección de datos personales: derecho fundamental del siglo xxi. Un estudio comparado. Boletín mexicano de derecho comparado. http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm Fecha de acceso 24 de octubre de 2014

Grupo Parlamentario Europeo. Comisión de Libertades Civiles, Justicia y Asuntos del Interior http://www.eppgroup.eu/es/libe

Himanen, Pekka. *La ética del hacker y el espíritu de la era de la información* http://www.educacionenvalores.org/IMG/pdf/pekka.pdf Fecha de acceso 27 de octubre de 2014.

http://www.opengovguide.com/standards-and-guidance/tshwane-principles-on-national-security-and-the-right-to-information/?lang=es Fecha de acceso 24 de octubre de 2014

Parlamento Europeo, *Informe sobre la vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos del Interior* (2013/2188(INI)). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//ES Fecha de acceso 24 de octubre de 2014.

Principios de Tshwane sobre Seguridad Nacional y Derecho a la Información. http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles

Fecha de acceso 24 de octubre de 2014

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. https://es.necessaryandproportionate.org/text Fecha de acceso 22 de octubre de 2014

Riva Palacio, Raymundo. Espionaje en México, una vieja historia. Periódico La Razón. http://www.razon.com.mx/spip.php?page=columnista&id_article=180583 Fecha de acceso 24 de octubre de 2014

Rosas, Israel. ONU: La vigilancia masiva requiere de controles que respeten los derechos humanos. http://www.fayerwayer.com/2014/07/onu-la-vigilancia-masiva-necesita-controles-que-respeten-dd-hh/. Fecha de acceso 24 de octubre de 2014

Sobre la mesa presunto espionaje de EE. UU. a México. http://diariojuridico.com.mx/actualidad/noticias/sobre-la-mesa-presunto-espionaje-de-ee-uu-a-mexico.html Fecha de acceso 24 de octubre de 2014.

The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. 30 June 2014 http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf Fecha de acceso 24 de octubre de 2014.

www.europol.europa.eu. Fecha de acceso 24 de octubre de 2014

www.opengovguide.com