Lecciones desde los Estados Unidos:
La necesidad práctica de los "Principios Internacionales de Vigilancia y Derechos Humanos"

Por: Hanni Fakhoury

Introducción

El objetivo de los Principios de Vigilancia y Derechos Humanos ("Principios") es brindar un marco de referencia a través del cual se puedan evaluar leyes, proyectos o prácticas actuales de vigilancia para asegurarse que sean consistentes con los derechos humanos. La elaboración de estos principios es una una oportunidad única para analizar la experiencia de los Estados Unidos en temas clave como la regulación de la vigilancia estatal y el acceso a los datos electrónicos.

Este documento busca presentar una breve explicación de las leyes en Estados Unidos en lo que respecta a cada uno de los Principios. Aunque las leyes en Estados Unidos se desarrollan tanto a nivel federal como estatal, este artículo se focaliza en la ley federal. Este documento también se concentra en las leyes en torno a las investigaciones nacionales, y sólo menciona brevemente lo relacionado con tareas de inteligencia exterior y asuntos de seguridad nacional.

Legalidad

En los Estados Unidos, la ley de vigilancia electrónica está contemplada en dos fuentes legales: (1) constitución federal o estatal; y (2) leyes federales o estatales.

La Cuarta Enmienda de la Constitución de los Estados Unidos se aplica al gobierno federal y a todos los estados, y prohíbe que el gobierno incurra en allanamientos y decomisos arbitrarios. Los organismos policiales deben obtener una "orden de allanamiento" antes de registrar un lugar, y eso incluye los dispositivos electrónicos y otras formas de almacenamiento de datos digitales. La Constitución define "allanamiento" como (1) el traspaso de la propiedad privada por el gobierno con el fin de obtener información, o (2) una intromisión del gobierno en un lugar donde una persona ha manifestado una expectativa subjetiva de intimidad que la sociedad acepta como razonable.

Bajo las leyes federales, la Ley de Privacidad de las Comunicaciones Electrónicas (Electronic Communications Privacy Act, ECPA) regula el acceso policial a diferentes formatos de datos electrónicos. La ECPA se ocupa de distintos formatos específicos de datos; El Título I es la Ley de Escuchas (Wiretap Act), que regula la forma en que el gobierno puede escuchar o interceptar el contenido de comunicaciones privadas, incluyendo conversaciones telefónicas. El Título II de la Ley ECPA es la Ley de Almacenamiento de las Comunicaciones (Stored Communications Act, SCA), que regula cómo el gobierno puede acceder al contenido de las comunicaciones electrónicas (como correos electrónicos, tweets, mensajes de texto, etc.), además de a otra información no vinculada con el contenido (como por ejemplo los registros de la ubicación de la torre de celular) desde un proveedor de comunicaciones electrónicas o de almacenamiento en la nube. Por último, las leyes de Pen Register/Trap and Trace Device (Pen/Trap) regulan cómo el gobierno puede obtener información de enrutamiento y transmisión de llamadas telefónicas y otras formas de contenido electrónico, como las direcciones IP o los encabezados de los correos electrónicos.

La mayoría de los estados han adoptado (en su totalidad o en parte) estas disposiciones de la ley federal. En general, los estados son libres de adoptar una mayor protección legal de la que existe en la legislación federal, pero no pueden proporcionar una menor protección de la privacidad. Algunos pocos estados han implementado algunas medidas para mejorar sus leyes de privacidad electrónica, y por lo general se han movido mucho más rápido que el gobierno federal, que no ha podido actualizar la Ley ECPA de forma adecuada desde que fue promulgada en 1986.

Necesidad

Bajo la Cuarta Enmienda, las órdenes de allanamiento debe limitarse tanto como sea posible para evitar revolver las pertenencias de una persona como medida general, algo que comprende sus datos electrónicos. Esto también incluye exigir que la Policía le entregue al juez un inventario de todo lo que ha incautado, para que el tribunal pueda supervisarlo. Cuando se trata de datos electrónicos, un tribunal ha advertido (PDF) que los jueces deben ejercer una "mayor vigilancia" para asegurar que el gobierno no esté recolectando más datos de los necesarios.

Sin embargo, a la hora de limitar el acceso policial las leyes de de privacidad electrónica en los Estados Unidos han tenido resultados dispares. La Ley de Escuchas contempla una fuerte protección a la privacidad, y requiere que la policía minimice las conversaciones telefónicas que intercepta para asegurarse de que sólo se están capturando las conversaciones que conciernen a una actividad criminal. Sin embargo, las leyes de SCA y Pen/Trap no incluyen requisitos similares de minimización de los contenidos de las comunicaciones electrónicas o de la información de enrutamiento de Internet. Esto debe ser modificado, en particular en el caso de la Ley SCA, que potencialmente podría otorgarle a la policía un amplio acceso a los correos electrónicos y a otras formas de contenido electrónico.

Idoneidad

Cómo se explica más arriba, y como ha demostrado el escándalo Petraeus, los agentes del orden en los EE.UU no se han restringido a la hora de registrar y de incautar datos electrónicos.

Por si fuera poco, ha existido una gran presión de los organismos policiales en el Congreso para implementar políticas de retención de datos para una amplia gama de datos almacenados por los proveedores de comunicación, como mensajes de texto y la información de la dirección IP. Estas políticas exigirían que los proveedores guarden la información únicamente para el uso de las

autoridades en un momento posterior, a menudo en contra de los deseos - y los intereses comerciales - de los mismos proveedores.

Es por esta razón que hay que luchar contra este tipo de políticas, que sirven sólo para el propósito gubernamental de vigilancia, y como se describe en más detalle a continuación, presentan riesgos para la seguridad.

Proporcionalidad

La Cuarta Enmienda de la Constitución de los EE.UU. requiere que la policía obtenga una "orden de allanamiento" para llevar a cabo un "registro" o para incautar datos electrónicos o físicos. Para obtener una "orden de allanamiento", la policía debe demostrar ante un juez que existe una "causa probable" - que es más probable que improbable - de que las pruebas de un delito se encuentran en el lugar que desea registrar. Si el juez cree que la policía ha demostrado esta causa probable, puede emitir la orden de allanamiento, aunque el magistrado debe especificar en qué lugares específicos la policía puede buscar y determinar cuáles son los elementos que puede incautar.

Sin embargo, este estándar de causa probable se aplica sólo si el gobierno está realizando un "allanamiento". Y hay muchas (de hecho demasiadas) excepciones al requisito de una orden de allanamiento. Por otra parte, si bien es evidente que la Cuarta Enmienda se aplica a los datos almacenados en los dispositivos físicos de una persona, como su teléfono celular, no está tan claro si también se aplica a los datos almacenados por terceros y en la nube.

Algunos tribunales han interpretado la Cuarta Enmienda en el sentido de que una persona no tiene una expectativa razonable de privacidad en la información que entrega a otra persona, como un proveedor de Internet o una red social. Esto implica que la policía no tendría la obligación constitucional de obtener una orden de allanamiento para conseguir información del cliente y datos de compañías como Facebook, Twitter o Google. Por ejemplo, un tribunal de Nueva York dictaminó que los fiscales no necesitaban tener una orden de allanamiento para obtener datos de Twitter acerca de Malcolm Harris, un manifestante de *Occupy Wall Street*, y que en su lugar podía obtener información como sus tweets, o dirección IP de inicio de sesión con una citación, ya que los datos pertenecían a Twitter, y no a Harris. Lo mismo ocurrió con los registros de Twitter de Birgitta Jonsdottir, diputada del Parlamento de Islandia, que el gobierno federal quería ver en relación a la investigación en curso sobre Wikileaks. Otros tribunales han estado en desacuerdo, entendiendo que aún si se le entrega a terceros información como el correo electrónico, esto sigue estando protegido por la Constitución y las fuerzas del orden deben obtener una orden de registro.

Para empeorar las cosas, las leyes federales tampoco utilizan este estándar de causa probable para todas las formas de almacenamiento de la información. En su lugar, en Estados Unidos se aplican diferentes estándares de protección de la privacidad a las diferentes formas de información electrónica y digital.

La protección más importante de la privacidad se encuentra en la Ley de Escuchas, que no sólo requiere que la Policía tenga una causa probable para creer que interceptando las llamadas telefónicas podrá probar un delito específico, sino que también requiere que las fuerzas del orden demuestren: (1) una causa probable de que mediante las escuchas se obtendrá información relacionada con un crimen, (2) que los procedimientos normales de investigación que se han intentado han fracasado o que razonablemente hubiera sido poco probable que tengan éxito si se hubieran intentado, o que son demasiado peligrosos, y (3) una causa probable para creer que el número de teléfono u otra

"infraestructura" electrónica en que ocurra la comunicación a ser interceptada tienen una conexión con el delito o con la persona a ser interceptada.

Pero las otras partes de la Ley ECPA no tienen las mismas fuertes protecciones a la privacidad contenidas en la Ley de Escuchas. La SCA sólo exige que la Policía obtenga una orden de allanamiento para acceder al contenido de las comunicaciones electrónicas almacenadas electrónicamente por menos de 180 días. Sin embargo, en el marco de la SCA se puede conseguir sin una orden de allanamiento acceder a las comunicaciones electrónicas más antiguas, así como otras formas de almacenamiento de datos electrónicos.

Si el gobierno puede demostrar ante un juez que existen "hechos específicos y objetivos" de que los datos son "relevantes y pertinentes para una investigación penal en curso" - un estándar inferior a la causa probable para una orden de allanamiento - la SCA le permite al gobierno obtener (1) el contenido de las comunicaciones electrónicas en almacenamiento electrónico de más de 180 días (por ejemplo, un correo electrónico antiguo en la bandeja de entrada); (2) el contenido de las comunicaciones electrónicas almacenadas en un proveedor de almacenamiento en la nube sin necesidad de previo aviso al abonado (como un PDF en Dropbox o en Google Drive); y (3) otros registros de clientes sin incluir el contenido (como información sobre la dirección IP o los registros de la ubicación de la torre de celular).

Y sólo con una citación –que no cuenta con ninguna supervisión judicial y que puede ser emitida por un abogado siempre que sea "relevante"–, el gobierno puede acceder a (1) el contenido de las comunicaciones electrónicas alojadas en un proveedor de almacenamiento en la nube, con previo aviso al cliente; y (2) otra "información sobre los abonados", incluyendo el nombre del cliente, dirección, registros telefónicos locales o de larga distancia, o los registros de tiempo de sesión y la duración, el tipo y la duración del servicio (incluyendo la fecha de inicio), número de teléfono u otra número o identidad del abonado, incluyendo cualquier dirección de red asignada temporalmente, y medios y fuente de pago por el servicio.

Por último, las leyes de Pen/Trap permiten que el gobierno obtenga información de enrutamiento si puede probar ante un juez que los datos que busca son "relevantes para una investigación criminal en curso".

Los diferentes estándares de estas leyes confunden a cualquiera. Los consumidores no están seguros de cuán protegida está su privacidad. Las agencias del orden, cómo se ha demostrado, son inconsistentes y poco claras al utilizar la ley en forma correcta para obtener los datos. Y, en este mundo moderno, los tribunales tienen dificultades para aplicar jurisprudencia de casos resueltos mucho antes de la llegada de tecnologías como los teléfonos celulares y las redes sociales.

Es necesario contar con un estándar uniforme que se aplique a todos los formatos de datos electrónicos y que contenga fuertes garantías de privacidad, como el que se recomienda en los Principios, para beneficiar por igual a los consumidores y a las agencias del orden.

Debido Proceso

Como ya se explicó anteriormente, no todas las solicitudes de la Policía para acceder a los datos electrónicos requieren autorización judicial previa. Y aun cuando la aprobación judicial es necesaria, los estándares para revelar información varían en función de los datos que se solicitan. Pero lo más problemático desde la perspectiva del "debido proceso" es la dificultad de probar violaciones de la ley tanto en contextos penales como civiles.

Un acusado en un caso penal puede accionar legalmente contra un allanamiento del gobierno y las incautaciones de datos electrónicos que se producen sin una orden de allanamiento (o con una orden de allanamiento deficiente). Lo más frecuente es que esto suceda después de que una persona ha sido acusada de un delito y presenta una moción para suprimir alguna evidencia. Pero la única evidencia que se puede suprimir es aquella que el gobierno tiene la intención de utilizar en contra del acusado en un juicio. Todo lo que una acción legal exitosa puede lograr es eliminar la capacidad del gobierno de utilizar ciertas formas de evidencia para condenar a la persona. Pero esa persona todavía puede ser procesada y encarcelada, en muchos casos, incluso sin el uso gubernamental de las pruebas. Y aunque los tribunales pueden "eliminar" la evidencia que se recolectó violando la Cuarta Enmienda, hay muchas excepciones al recurso de la supresión que disminuyen su eficacia. Por ejemplo, si la evidencia fue descubierta por agentes que actuaron de buena fe -en la creencia razonable, pero equivocada, de que estaban autorizados a confiscar el elemento-, esta no se eliminará. Además, los tribunales son reacios a dudar de la policía o sus colegas en la justicia a la hora de reveer el proceso de allanamiento y de incautación. En consecuencia, la supresión de evidencia no es algo muy común.

La situación es aún menos prometedora cuando se trata de demostrar violaciones a las restricciones legales sobre el acceso del gobierno a los datos electrónicos. Ni la Ley de Escuchas, ni la SCA o Pen/Trap contienen un remedio de supresión legal para la incautación ilegal de los contenidos de las comunicaciones electrónicas o de la información de enrutamiento, y esto debe plantearse en el marco de la Cuarta Enmienda y no de las leyes en sí mismas.

Para las personas que han sido vigiladas ilegalmente sin ser acusadas de un delito, tanto la Ley de escuchas y la SCA permiten que un privado pueda iniciar acciones legales por intercepciones de audio e incautaciones de contenidos electrónicos inadecuadas. Pero aunque sea difícil superar los muchos obstáculos procesales para presentar una demanda civil contra el gobierno, es algo posible. Por ejemplo, generalmente se necesitará demostrar que la violación fue intencional, algo que puede ser difícil de probar. En los casos de incautaciones ilegales, la EFF ha recurrido en algunas oportunidades a la Ley de Protección de la Privacidad (Privacy Protection Act) -que limita la capacidad del gobierno para buscar o apoderarse de los elementos relacionados con la publicación de un periódico, revistas u otras publicaciones, para demandar al gobierno.

A veces, los asuntos de seguridad nacional pueden presentar una barrera difícil. La EFF ha demandado tanto a la Agencia de Seguridad Nacional (NSA, por su sigla en inglés) y a AT&T por el programa del gobierno federal de escuchas telefónicas sin orden judicial que comenzó durante la presidencia de George W. Bush y que tuvo variados niveles de éxito. El caso en contra de la NSA se ha movido lentamente, con el gobierno tratando de conseguir que el caso se desestime porque el litigio obligaría a revelar "secretos de Estado". Y el Congreso aprobó una ley que le otorga inmunidad judicial a AT&T, poniendo efectivamente un punto final a cualquier acción legal que discuta su papel en el programa de escuchas telefónicas sin órdenes judiciales.

Notificación al usuario

La ley federal permite que las agencias del orden exijan que los proveedores mantengan en silencio las solicitudes de los datos de clientes. Por ejemplo, como parte del Acta PATRIÓTICA post 9/11, el FBI puede eludir a los tribunales y emitir cartas administrativas bajo su propia órbita, llamadas Cartas de Seguridad Nacional (PDF) (NSLs, por su sigla en inglés), y enviarlas a las empresas de telecomunicaciones. Las NSLs no sólo exigen que las empresas revelen información acerca de un cliente, sino que también requieren que las compañías no informen al cliente de ese pedido, manteniendo en secreto incluso la

recepción de una de estas cartas. Sólo ha habido un pequeño número de acciones legales contra esta práctica. Incluso fuera del contexto de Seguridad Nacional, la SCA permite al gobierno retrasar el aviso a un usuario sobre una solicitud del gobierno de acceder a los contenidos de las comunicaciones electrónicas por un máximo de 90 días. Además, existe la posibilidad de solicitar una prórroga adicional de 90 días.

En ausencia de cualquier limitación legal de la capacidad de un proveedor de servicios de notificar a sus usuarios de estas solicitudes de datos, las empresas tienen un historial dispar a la hora informar a sus clientes. Twitter, por ejemplo, tiene la política de comunicar a sus usuarios sobre todas las solicitudes de información antes de divulgar los datos, a menos que esté prohibido por orden judicial. La política de Facebook es más imprecisa, dando a entender que la policía debe obtener una orden judicial para evitar la notificación, pero también permitiendo no revelar la información si esto "diera lugar a un riesgo de daños".

No se debe subestimar la importancia de las notificación a los usuarios, quienes deben saber acerca de las solicitudes sin demora para salvaguardar sus datos y solicitar asistencia jurídica y orientación. Cualquier solicitud gubernamental para demorar la notificación debe limitarse a circunstancias de emergencia, y este plazo debe ser lo más corto posible. Debe rechazarse el mecanismo secreto de las NSLs, de acceso vedado a los datos de un usuario. También debe rechazarse el enfoque de la SCA de largos períodos de notificación tardía. Al instaurar este tipo de normas para las agencias del orden, se alentará a que las empresas informen a sus usuarios de las solicitudes de aplicación de las autoridades con mayor frecuencia que la actual.

Transparencia en la vigilancia del gobierno

La ley de EE.UU. está totalmente ausente cuando se trata de la transparencia. Con la excepción de las órdenes de interceptación bajo la Ley de Escuchas, para lo cual el gobierno debe publicar un informe anual sobre el uso de las escuchas telefónicas, existe muy poca transparencia sobre la frecuencia con la que el gobierno trata de acceder a las pruebas electrónicas (e incluso el Departamento de Justicia ha estado bajo la lupa por no entregar al Congreso registros y estadísticas completos de la Ley de Escuchas, como lo requiere la ley). Pero más allá de las órdenes de escuchas, hay poca transparencia por parte del gobierno o de los proveedores de la cantidad de información que el gobierno está recolectando, y con qué fines.

En consecuencia, la información sobre el uso gubernamental de los diversos formatos de datos electrónicos sólo ha salido a la luz a través de una demanda del Congreso para obtener información sobre las solicitudes a las compañías de telefonía celular o de una solicitud de acceso a la información presentada por la Unión Americana de Libertades Civiles (ACLU, por su sigla en inglés) a la Policía que exigía información sobre la utilización de los datos de los registros de la ubicación de la torre de celular. También existe más información gracias a los informes elaborados por empresas como Google y Twitter sobre el número de solicitudes nacionales e internacionales del gobierno sobre datos del usuario. Lamentablemente, estos informes son la excepción, y no la regla. La mayoría de las empresas de tecnología no revelan voluntariamente estos datos. Y los intentos a nivel estatal para exigir que así lo hagan se han encontrado con una fuerte oposición de las empresas.

En definitiva, lo que demuestran estas peticiones informales es que las solicitudes del gobierno para acceder a datos de los usuarios están en aumento. Por lo tanto, es necesaria una mayor transparencia para permitir que los usuarios vigilen a estas crecientes demandas y para prevenir los abusos.

Supervisión

En los Estados Unidos, la supervisión presumiblemente proviene de distintas ramas del gobierno. Los organismos policiales dentro de la rama ejecutiva cuentan con inspectores generales que revisan las prácticas internas, mientras que las agencias de seguridad nacional reportan al Director de Inteligencia Nacional. En el poder legislativo, los comités de supervisión del Congreso reciben los informes de los diferentes organismos policiales. Y la rama judicial recibe las acciones legales contra la vigilancia del gobierno.

Pero ninguno de estos comités de vigilancia es verdaderamente independiente. Incluso los comités supuestamente "independientes" no lo son en sentido literal. Por ejemplo, la Junta de Supervisión de Inteligencia (IOB, por su sigla en inglés) es una junta independiente de supervisión civil, cuyos miembros son designados por el Presidente, que tiene la misión de asegurar que el gobierno cumple con la ley durante las investigaciones de inteligencia exterior. Sin embargo, sus acciones, e incluso por un tiempo sus miembros, están bajo un manto de secreto. A nivel de inteligencia nacional, se creó la Junta de Vigilancia de Derechos Civiles y Privados (PCLOB, por su sigla en inglés) con la intención de actuar como una institución de control independiente de las prácticas de vigilancia domésticas. Pero esta junta ha sido en gran medida ineficaz, abandonada tanto por los presidentes Bush y Obama, y, a pesar de su relativamente corta existencia, ya fue reorganizada (PDF). Tanto la IOB como la PCLOB existen dentro (y responden) a la oficina del presidente, con lo que su verdadera "independencia" plantea serias dudas.

Así, además de los esfuerzos de varias organizaciones de libertades civiles como la EFF, ACLU, Center for Democracy and Technology (CDT) y el Electronic Privacy Information Center (EPIC), entre otros, que buscan dar cuenta de las prácticas de vigilancia del gobierno a nivel nacional, no existe ningún comité efectivo, público y de supervisión independiente encargado de examinar las prácticas nacionales. Y, por supuesto, a pesar de sus mejores esfuerzos, estas organizaciones están limitadas en cuanto a la información a la que pueden acceder. La mayor parte de los datos se obtienen gracias a procesos judiciales y solicitudes de acceso a la información, y estas organizaciones no están ciertamente en condiciones de examinar, en la mayoría de los casos, información secreta o clasificada.

Para evitar abusos de las libertades civiles y arrojar una mayor transparencia sobre las prácticas de gobierno es necesario que exista un comité de supervisión más formal y verdaderamente independiente, que se encargue de revisar tanto las prácticas de vigilancia a nivel nacional como internacional y las tareas de inteligencia.

Integridad de las comunicaciones y los sistemas

Para contar con un mundo digital seguro es fundamental la integridad de la arquitectura de la red. Sin embargo, el gobierno de EE.UU. ha librado una larga batalla en aparente contradicción con este objetivo. A pesar de los evidentes riesgos para la seguridad y la privacidad, ha instado al Congreso a implementar largos períodos obligatorios de retención de datos, empujados por la prohibición del cifrado- una herramienta crucial para proteger las comunicaciones electrónicas -y todo mientras hacía lobby para garantizar el acceso, asegurándose la existencia de su propia puerta trasera en los sistemas de comunicación.

La propuesta de una puerta trasera en las comunicaciones por Internet proviene de un esfuerzo para actualizar el Programa de Asistencia para el Cumplimiento de la Ley de Comunicaciones (Communications Assistance for Law Enforcement Act, CALEA). En 1994, el Congreso aprobó CALEA, obligando a las compañías telefónicas a rediseñar sus arquitecturas de red para facilitar las escuchas telefónicas. Pero esto excluía específicamente los datos que viajan a través de Internet. A medida que se

expandió el uso de la web, las agencias del orden han aplicado una creciente presión sobre el Congreso para actualizar CALEA y exigir a los proveedores que aseguren que sus redes de comunicación tienen una puerta trasera que también permita al gobierno interceptar las comunicaciones por Internet. Esta actualización propuesta a CALEA (más que nada como una demanda policial de retención de datos) tiene evidentes consecuencias negativas de largo alcance para la privacidad, la seguridad y la innovación.

Por otra parte, hubo momentos en que el gobierno aplicó mano dura a individuos que dejaron en evidencia vulnerabilidades de seguridad y fallas. Un investigador fue recientemente condenado por un delito federal que prohíbe el acceso ilegal a una computadora, cuando reveló un error en la página web de AT&T. Este error le permitió obtener las direcciones de correo electrónico de los usuarios de iPad de AT&T con sólo visitar un sitio web sin restricciones, y sin pasar por las barreras tecnológicas para acceder a esos datos. En otro caso, la Autoridad de Transporte de Massachusetts intentó silenciar a un grupo de investigadores que tenían previsto presentar en una conferencia un trabajo acerca de las vulnerabilidades que descubrieron en el sistema de pago de tarifas de tránsito.

Básicamente, el gobierno debería alentar a las empresas de tecnología para que mantengan los datos de sus clientes de forma segura. Sin embargo, al minimizar el riesgo de divulgación también se debe prohibir que el gobierno acceda a esta información por una puerta trasera y se debe limitar la retención de datos. Al mismo tiempo, los investigadores de seguridad que no acceden a la información electrónica de forma ilegal no deberían ser tratados como criminales simplemente por informar al público sobre sus hallazgos.

Garantías para la cooperación internacional

Lamentablemente, muchos países han tratado de exportar algunas de las peores prácticas de vigilancia de los Estados Unidos. Y, desafortunadamente, estos países han utilizado la cooperación internacional como un medio para vigilar a los ciudadanos, violando sus respectivas leyes internas. Por ejemplo, en la investigación penal de los EE.UU. de la página web de Megaupload y su fundador Kim Dotcom por infracción de derechos de autor, se descubrió que las autoridades de Nueva Zelanda no sólo obtuvieron órdenes de allanamiento incorrectas para la casa de Doctom pero que también lo habían espiado ilegalmente mediante el control de todo el tráfico de Internet que entraba y salía de su casa.

Es por ello que es importante asegurarse de que cualquier ley o tratado que legitima la vigilancia masiva deba ser cuestionado. Y todo tratado de asistencia legal mutua (MLAT, por su sigla en inglés) debe asegurar que frente a leyes en conflicto se aplicará aquella norma que ofrezca mayores garantías.

Prevenir el acceso ilegítimo

Como se ha explicado anteriormente, en contextos de carácter no penal, las personas que han sido víctimas de vigilancia ilegal disponen de recursos tanto bajo la Ley de Escuchas y la SCA para iniciar acciones legales. Pero los tribunales y las legislaturas deberían asegurarse de que no existen barreras excesivamente onerosas para demandar.

Costos de vigilancia

Poco se sabe sobre el costo de la vigilancia que ejerce el gobierno en los EE.UU., aún cuando los proveedores de servicios han insistido reiteradamente en que no están obteniendo ganancias de los organismos policiales y que sólo están recuperando los costos. Un completo pedido de acceso a la información de la ACLU en 2012 reveló en detalle los precios que las empresas cobran para que los organismos policiales accedan a las escuchas telefónicas y los registros de la ubicación celular, revelando

que las sumas que cobran los proveedores varían, y que muchos no le cobran nada a los organismos en respuestas a situaciones de emergencia.

Asegurarse que los organismos policiales son responsables de los costos de la vigilancia puede en muchos casos servir como un estandarte contra el abuso del gobierno: cuanto más oneroso sea obtener los registros electrónicos y contenidos, más cuidadoso será el gobierno en sus búsquedas.

Conclusión

Esperemos que este manual básico de la ley en EE.UU. demuestre la importancia práctica de los Principios. Como ponen de manifiesto los errores de la legislación estadounidense, hay muchas maneras en que la privacidad puede ser erosionada y la vigilancia irrestricta puede prosperar. Los Principios constituyen un primer paso, algo crucial no sólo para asegurarse que la privacidad electrónica se desarrolle a nivel internacional, sino también para comenzar a llenar los agujeros legales en las normas de EE.UU en cuanto a la protección de la privacidad.