Evaluación de la legalidad y proporcionalidad de la vigilancia de las comunicaciones en la legislación de Estados Unidos

Por Mark Rumold, abogado de EFF

Marzo 2016

ELECTRONIC FRONTIER FOUNDATION

Tabla de contenidos

I.

Introducción

Si bien la privacidad es un componente básico en la legislación de Estados Unidos, las nuevas tecnologías generan dudas en cuanto a las circunstancias en las cuales los ciudadanos estadounidenses pueden confiar en que sus datos estarán a salvo de ser accedidos por el gobierno. Este reporte da comienzo al análisis y al debate sobre la legislación y las prácticas de vigilancia de Estados Unidos, medidos en función de dos principios clave de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[1] El documento de los 13 Principios fue elaborado por expertos en derecho de todas partes del mundo para poner en claro cómo el derecho internacional de los derechos humanos se aplica en el contexto digital actual, particularmente en vista del incremento y los cambios en las tecnologías y técnicas de vigilancia de las comunicaciones. Los Principios se encuentran firmemente arraigados en el consolidado derecho internacional de los derechos humanos. En especial, se basan en los derechos a la privacidad, a la libertad de opinión y expresión, y a la libertad de asociación, garantizados en los instrumentos internacionales sobre derechos humanos.

Pese a que este reporte no brinda una cobertura exhaustiva sobre todas las leyes estatales y federales que regulan la vigilancia de las comunicaciones en Estados Unidos, sí se identifican y abordan temas importantes que se encuentran presentes en la legislación sobre vigilancia estadounidense. Específicamente, este documento examina cómo la Constitución de Estados Unidos así como también una serie de leyes federales y estatales abordan los valores de Legalidad y Proporcionalidad detallados en los Principios de Necesidad y Proporcionalidad.

En primer lugar, el advenimiento de nuevas tecnologías ha creado, lamentablemente, incertidumbres en lo concerniente a la aplicación de la legislación de Estados Unidos a las prácticas de vigilancia modernas. Adicionalmente, algunas leyes desactualizadas y la aplicación intrincada de leyes anteriores dan lugar a una situación en la que la normativa estadounidense no cumple con los estándares de claridad y precisión que se describen en el Principio de Legalidad.

Además, a pesar de que el Principio de Proporcionalidad se ve reflejado de manera teórica tanto en el derecho constitucional como las leyes comunes, el uso que hace el gobierno de las nuevas tecnologías de vigilancia, en la práctica va en contra de este principio. Una vez más, el resultado es la violación generalizada del Principio de Proporcionalidad, inclusive en la

recolección de datos masiva de la Agencia de Seguridad Nacional (NSA) y en las poderosas herramientas de vigilancia utilizadas por las agencias locales de aplicación de la ley.

Aun mientras los tribunales luchan para llegar a un consenso sobre cómo se aplicarán las leyes desactualizadas a las nuevas tecnologías de vigilancia, algunas legislaturas estatales se enfocan en innovaciones para proteger la privacidad de sus ciudadanos. En definitiva, para crear un estándar unificado para el acceso por parte del gobierno a una serie de distintos tipos de datos electrónicos, sea quizás necesario que el Congreso de Estados Unidos adopte reformas integrales en cuanto a la vigilancia de las comunicaciones.

II.

El Principio de Legalidad

El primero de los Principios de Necesidad y Proporcionalidad es el de "Legalidad". Este principio dispone que cualquier limitación a los derechos humanos debe ser prescrita por ley. Específicamente, el Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficiente para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Como explicó el Tribunal Europeo de los Derechos Humanos (TEDH), "en primer lugar, la ley debe ser suficientemente accesible: el ciudadano debe ser capaz de tener una indicación de qué es adecuado en las circunstancias de las normas legales aplicables a un caso concreto. En segundo lugar, una norma no puede ser considerada como una 'ley' a menos que esté formulada con la suficiente precisión para permitir al ciudadano regular su conducta; debe ser capaz—si es preciso con un asesoramiento adecuado—de prever, en un grado que sea razonable a las circunstancias, las consecuencias de un determinado acto".[2] Así, el principio de "legalidad" exige que las leyes sean claras, públicas, y estén sujetas a supervisión, y que dichas leyes no otorguen excesiva discrecionalidad a los funcionarios públicos.[3]

Por lo general, la legislación interna de EE. UU. tiene su origen en dos fuentes: (1) en la constitución federal y en las estatales; y (2) en el derecho federal o las leyes comunes. Hasta hace poco, tanto las leyes constitucionales federales y estatales como las leyes comunes estaban atrasadas con respecto a los avances tecnológicos. Como esta situación se relaciona con el Principio de Legalidad, los ciudadanos se veían en desventaja, sin ser capaces de regular de manera eficaz sus conductas o de entender con certeza el proceso legal que el gobierno debe seguir antes de tener acceso a información sensible protegida o antes de llevar a cabo procedimientos de vigilancia electrónica. Pero durante los últimos años, los tribunales y órganos legislativos tanto a nivel federal como estatal se han involucrado de una manera más activa en la regulación de la vigilancia electrónica. Algunos incluso extendieron las protecciones para la privacidad de los ciudadanos de nuevas maneras.

A. El Principio de Legalidad en la legislación de Estados Unidos

Protecciones constitucionales

La fuente de regulación de vigilancia electrónica más importante es la Cuarta Enmienda a la Constitución de los Estados Unidos, la cual prohíbe al gobierno participar en allanamientos y confiscaciones injustificadas. Esto hace que la aplicación de la ley deba obtener una "orden de allanamiento" previa al registro de un lugar, inclusive de aparatos electrónicos y otras formas de almacenamiento de datos digitales. La Cuarta Enmienda define un "allanamiento" de dos maneras: (1) la invasión a propiedad privada por parte del gobierno con el propósito de obtener información; o (2) una intromisión del gobierno en un lugar en el que una persona espera privacidad, expectativa que la sociedad consideraría razonable.[4] La Cuarta Enmienda es el punto de partida; los estados y el gobierno federal están facultados para brindar mayor protección para los ciudadanos a través de la legislación o de las constituciones estatales.[5]

Debido a que la Corte Suprema de EE. UU. —el máximo tribunal del derecho constitucional de Estados Unidos—únicamente decide sobre unos pocos casos cada año, se utilizan casos análogos para resolver cuestiones más modernas de allanamiento y confiscación.

Por ejemplo, en los años setenta, la Corte Suprema de EE. UU. dictaminó que la policía podía, después de arrestar a un individuo, registrar los objetos encontrados en su posesión, como un paquete de cigarrillos, sin haber obtenido una orden judicial o sin que exista sospecha individualizada contra aquella persona.[6] Cuando los teléfonos celulares se convirtieron en objetos cotidianos hacia fines del siglo XXI, el gobierno sostenía sistemáticamente que estos teléfonos equivalían a un paquete de cigarrillos, y que la policía tenía la libertad de hurgarlos a su antojo. Los tribunales inferiores expresaron opiniones encontradas acerca de este asunto, lo que resultó en reglamentaciones diferentes en las distintas partes del país.[7]

En el 2014, este tema se resolvió de manera definitiva cuando la Corte Suprema de EE. UU. falló en el caso *Riley v. California*, 134 S.Ct. 2473 (2014), en el que determinó que la policía tenía prohibido registrar los datos de un teléfono celular de una persona que haya sido arrestada sin contar con una orden judicial. El caso *Riley* desestimó como "forzado" el intento de considerar un teléfono celular equivalente a un objeto físico, como lo es un paquete de cigarrillos. En cambio, la Corte llevó a cabo un análisis independiente acerca de la naturaleza de los datos digitales y concluyó que los problemas de privacidad eran más que

suficientes para exigir que la policía obre bajo órdenes. La sentencia se enfocó específicamente en que los datos digitales son cualitativa y cuantitativamente diferentes de los objetos físicos y determinó que una norma que permita registrar un paquete de cigarrillos no podía extenderse a los datos de un teléfono celular.

El caso *Riley* es un modelo a seguir para que los tribunales puedan asegurar que la vigilancia se lleva a cabo cumpliendo con los estándares provistos por el Principio de Legalidad. Esta decisión, accesible al público, creó una regla clara que no brindó excesiva discrecionalidad a los funcionarios del gobierno. En su lugar, le proporcionó al gobierno un marco estandarizado para el acceso a los datos digitales de las personas bajo arresto—con el uso de una orden de allanamiento—y concientizó a los ciudadanos acerca de sus derechos a la privacidad.

Los demás tribunales deberían seguir los pasos de *Riley* y crear reglas que el gobierno pueda seguir con facilidad y que los ciudadanos puedan comprender.

El enfoque de *Riley* está implicado en otras herramientas tecnológicas a disposición de la policía. Por ejemplo, actualmente existe un debate en EE. UU. sobre si la policía debe obtener una orden de cateo para acceder a la información histórica que recolectan las torres de telefonía, es decir, el registro de una torre en particular a la cual se conecta el celular los cuales están en posesión del proveedor de telefonía móvil. Estos datos sensibles pueden revelar la ubicación física de una persona durante un periodo de tiempo extendido, creando una imagen privada de todos los lugares a los que viaja el propietario del teléfono celular. En los años setenta, la Corte Suprema de los Estados Unidos decidió que no había derecho a la privacidad en los registros en posesión de terceros, incluidos los registros de los números que marca una persona.[8] El gobierno ha usado este antecedente análogo para argumentar que tampoco existe el derecho a la privacidad en los registros de ubicación de un teléfono celular, a pesar de que los registros de ubicación de los teléfonos son más reveladores que el relativamente simple registro de números marcados revisados por la Corte en los años setenta.

Mientras que la Corte Suprema de EE. UU. todavía no se ha pronunciado con respecto a este asunto en particular, al menos una jueza ha señalado que es hora de "reconsiderar la premisa de que un individuo no tiene expectativas de privacidad sobre información divulgada a terceros" ya que "este enfoque no es apropiado para la era digital, en la que las personas revelan una gran cantidad de información sobre sí mismas a terceros mientras llevan a cabo tareas mundanas".[9] Desde el 2013, los tribunales superiores de tres estados—Massachusetts, Nueva Jersey, y Florida—adoptaron el modelo de análisis de la Corte en el caso *Riley* y determinaron que la policía debe contar con una orden para obtener

información almacenada sobre localización a través de torres de telefonía.[10] Como en *Riley*, estos tribunales se enfocaron en la esencia cuantitativa y cualitativa de la información procurada por el gobierno al determinar la protección legal que aplicaría a sus casos. Y todos los tribunales acordaron seguir una regla clara—exigir una orden, basada en una sospecha fundada—en lugar de utilizar un examen ad hoc y multifactorial de difícil aplicación práctica para los oficiales y que sería también de difícil comprensión para el público.

Protecciones Jurídicas

Dentro de Estados Unidos, las protecciones constitucionales son sólo un punto de partida; tanto los órganos legislativos a nivel federal como a nivel estatal pueden ir más allá de lo que establece la Constitución, y brindar una protección incluso mayor.

De hecho, el Congreso de EE. UU. hizo lo propio en 1986 al aprobar la Ley de Privacidad en las Comunicaciones Electrónicas (ECPA, por sus siglas en inglés), destinada a brindar protección legal para los datos electrónicos y los registros generados por dispositivos electrónicos y almacenados por los proveedores de servicios. La ley ECPA respondió a las decisiones de la Corte Suprema de EE. UU. de los años setenta, en las que determinaba que no había derecho a la privacidad en los registros en posesión de terceros; el Congreso decidió establecer protecciones para la privacidad al percibir la ausencia de protección constitucional. Sin embargo, desde su promulgación en los años ochenta, la ley ECPA no sufrió ninguna reforma para abordar la tecnología moderna, lo que deja un vacío en la protección de la privacidad.

Esto se observa más gráficamente en el trato que da la ley ECPA a los contenidos de comunicaciones electrónicas como los emails o los mensajes de texto. En virtud de la ley ECPA, el gobierno debe utilizar una orden para obtener los contenidos de las comunicaciones electrónicas a través de los proveedores de servicios si el mensaje se encuentra almacenado de manera electrónica por hasta 180 días.[11] Sin embargo, una vez que el almacenamiento sobrepasa los 180 días, la ley no deja en claro si es necesario contar con una orden, y el gobierno puede así intentar obtener los mensajes a través de un proceso más corto.[12] Esta línea divisoria marcada por el periodo de 180 días es un vestigio de esa época: en los años ochenta, el almacenamiento en línea era escaso y el Congreso supuso que la mayoría de las personas iban a descargar los mensajes importantes en sus computadoras—lo cual está protegido por la Cuarta Enmienda—y todos los mensajes que todavía estuvieran almacenados de manera electrónica después de un lapso de 6 meses se consideraban completamente abandonados. Hoy en día, usamos los e-mails de manera muy diferente: el advenimiento de la computación en la nube y los teléfonos inteligentes nos ha llevado a almacenar los mensajes en línea para poder tener acceso a ellos desde cualquier lugar, en vez de descargarlos en computadoras. Lamentablemente, el Congreso no ha actualizado la ley

ECPA desde los años ochenta. Así, la forma en la que usamos los e-mails ha cambiado drásticamente, pero la ley no ha podido estar a la altura.

A nivel estatal, muchos de los estados han promulgado leyes que brindan mayores protecciones para la privacidad que las de la ley ECPA.[13] Algunos implementaron leyes que exigen a la policía poseer una orden judicial para obtener los contenidos de comunicaciones electrónicas—sin prejuicio del tiempo que lleven almacenados.[14] Otros aprobaron leyes que requieren una orden judicial antes de que la policía comience a rastrear la ubicación de una persona a través de su celular.[15]

Es notable que en el 2015 el estado de California aprobara la reforma de una ley general sobre vigilancia. Al descartar el mosaico de leyes que previamente habían regulado el acceso de los órganos de aplicación de la ley a información personal en California, la nueva ley impone la necesidad de una orden unificada para acceder a una variedad de información protegida. Actualmente, por ejemplo, para obtener e-mails, mensajes de texto, o cualquier documento privado almacenado por un tercero, la policía debe obtener una orden emitida por un juez imparcial. El mismo requisito de contar con una orden judicial aplica a la información sobre la ubicación de una persona y a los "metadatos" de las comunicaciones electrónicas. [16]

B. Áreas de la legislación de EE. UU. que requieren desarrollar más profundamente el Principio de Legalidad

El Principio de Legalidad requiere acceso público a las leyes que rigen a la vigilancia, pero la legislación sobre la vigilancia electrónica en Estados Unidos está plagada de secretismo. Este es el caso también tanto para la vigilancia para la seguridad nacional como para aquella llevada a cabo con propósitos de aplicación de la ley interna. Si bien existe un gran número de principios constitucionales en la legislación de EE. UU. que garantizan a los ciudadanos el acceso y el entendimiento de la ley,[17] dichos principios se respetan más en el incumplimiento en el contexto de la vigilancia electrónica.

En primer lugar, en el contexto de la seguridad nacional, el poder ejecutivo invoca su poder de "clasificación"[18] para hacer que las opiniones legales o decisiones judiciales concernientes a la vigilancia no sean reveladas al público. En 1978, Estados Unidos creó un tribunal especializado, el Tribunal de Vigilancia de Inteligencia Extranjera ("FISC", por sus siglas en inglés), para escuchar las peticiones del gobierno en relación con la vigilancia con fines de seguridad nacional.[19] Después de los atentados del 11 de septiembre del 2001, el gobierno comenzó a solicitar al tribunal FISC poderes cada vez más agresivos para poder llevar a cabo tareas de vigilancia dentro de Estados Unidos. Debido a que los procedimientos del FISC eran confidenciales y *ex parte*, el gobierno logró convencer al tribunal de autorizar una serie

de programas de vigilancia de legalidad dudosa.[20] Y, debido a las aseveraciones sobre clasificación del poder ejecutivo, las opiniones legales se mantuvieron en secreto hasta el 2013 —momento en que el gobierno desclasificó muchas de las decisiones tomadas por el tribunal FISC a la luz de las revelaciones de Edward Snowden. La Ley Libertad de EE. UU. (*Freedom Act*), un conjunto de reformas sobre seguridad nacional aprobadas en 2015, abordó este problema: la nueva norma requiere que el gobierno desclasifique y publique cualquier interpretación legal "significativa" del tribunal FISC.[21] Si bien las decisiones del tribunal FISC ahora deben divulgarse, algunos programas de vigilancia de seguridad nacional no se autorizan a través de los tribunales, y, así, sus análisis jurídicos (si es que hay alguno) permanecen ocultos dentro del poder ejecutivo.

Las interpretaciones legales secretas que autorizan nuevas técnicas de vigilancia son también un problema en las investigaciones de los órganos nacionales encargados de hacer cumplir la ley. Por lo general, los fiscales y los funcionarios del orden público realizan una petición a los juzgados o a los jueces de primera instancia, *ex parte*, para que emitan órdenes para la autorización de la vigilancia. El gobierno habitualmente solicita que tales peticiones sean secretas y no estén disponibles al público con el fin de que aquellos que sean investigados no se alerten del hecho de que se llevará a cabo tal investigación. Aunque esto parece lógico, surgen problemas en las siguientes situaciones: (1) cuando las solicitudes de vigilancia nunca se hacen públicas, y (2) cuando el uso de las técnicas de vigilancia no se da a conocer, incluso cuando puede ser de ayuda en un proceso penal.[22] Estos factores hicieron que las técnicas de vigilancia de los órganos de aplicación de la ley estén ocultas—como el uso de recolectores IMSI (*IMSI catchers*) o software malicioso (*malware*) perteneciente al gobierno—del escrutinio público y de la impugnación jurídica.

El Principio de Legalidad también exige claridad, y el enfoque de la vigilancia de las comunicaciones de Estados Unidos—en general—dista mucho de ser claro. Como se describió anteriormente, el conjunto de leyes que regula el acceso a los datos varía en razón de, al menos, los siguientes factores:

(1) si se trata de una investigación estatal o federal;

(2) si el estado adoptó normas más protectoras para la regulación del acceso a la información;

(3) si la investigación se lleva a cabo con propósitos de aplicación de la ley o con propósitos relacionados con la inteligencia;

(4) si la información que se pretende encontrar tiene carácter de "contenido" o de "metadato";

(5) si la información que se pretende encontrar se encuentra "almacenada" o se adquiere en "tiempo real"; y

(6) si la información se encuentra bajo la custodia de un tercero.

Cualquiera de estos factores, ya sea que se tomen individualmente o en conjunto, puede afectar la posibilidad de que se solicite una orden judicial para tener acceso a datos y también al estándar pertinente que el gobierno debe cumplir para tener acceso a la información.

El enfoque fragmentario que toma Estados Unidos se origina de la ausencia de legislación federal o de acción judicial que cree un estándar claro y coherente a escala nacional. Por ejemplo, el hito legislativo que se aprobó en el estado de California aplica únicamente para las agencias de aplicación de la ley de California. Los demás funcionarios estatales o federales que quieran acceder a la misma información que las agencias de aplicación de la ley de California pueden estar habilitados a hacerlo mediante diferentes estándares legales y siguiendo diferentes procesos legales. Aunque se ha pedido una reforma completa de las leyes de vigilancia, por ahora ninguna ha logrado pasar por los dos cuerpos del Congreso de EE. UU.

Hasta que se adopte este enfoque integral, las leyes que regulan el acceso a la información personal en todo Estados Unidos seguirán siendo poco claras.

III.

El Principio de Proporcionalidad

El segundo principio que abordaremos en este trabajo es el de "Proporcionalidad". Según este principio, la vigilancia de las comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos y que amenaza los cimientos de una sociedad democrática. Las decisiones sobre la vigilancia de las comunicaciones deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia.

Este análisis exige, al menos, que el estado establezca:

(1) que existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo[23] ha sido o será llevado a cabo;

(2) que existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la Información Protegida[24];

(3) que otras técnicas de investigación menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada resultaría la menos invasiva en la práctica;

(4) que la información a la que se accederá estará limitada a lo relevante y material para el delito grave o la amenaza específica al fin legítimo alegado;

(5) que cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud;

(6) que la información será accedida sólo por la autoridad especificada y usada solamente para el propósito y durante el lapso para los cuales se otorgó la autorización; y

(7) que las actividades de vigilancia solicitadas y las técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

Nuevamente, dentro de Estados Unidos, el Principio de Proporcionalidad se ve reflejado de manera tradicional tanto en el derecho constitucional como en las leyes comunes. En efecto, los intereses protegidos por el Principio de Proporcionalidad están profundamente integrados en la constitución federal y en las estatales; y muchas leyes sobre vigilancia electrónica brindan protecciones similares a las que se contemplan en este Principio. Sin embargo, la nueva tecnología de vigilancia y el incremento en la cantidad de datos

disponibles a través de la vigilancia de las comunicaciones hicieron difícil la aplicación de estos Principios, lo que trae como consecuencia la falta de proporcionalidad en algunas actividades de vigilancia por parte del gobierno.

A. El Principio de Proporcionalidad en la legislación de Estados Unidos

Protecciones Constitucionales

La piedra de toque de la Cuarta Enmienda—como describimos anteriormente, la enmienda constitucional federal más importante en el contexto de la vigilancia de las comunicaciones —es la "razonabilidad".[25] En general, se presume que los registros llevados a cabo sin una orden que representan una intrusión en la expectativa razonable de privacidad de una persona son desproporcionados, y por lo tanto, están prohibidos.[26] El requisito de contar con una orden asegura la aplicación de muchas de las protecciones consagradas en el Principio de Proporcionalidad.

En primera instancia, una orden para realizar un registro o una confiscación puede ser emitida sólo teniendo una "sospecha fundada".[27] Esto significa que los funcionarios del gobierno deben brindar información convincente que permita al juez de control llegar a la conclusión de que hay probabilidades de que el registro aporte evidencia de un crimen.[28] El requisito de "sospecha fundada" es similar a las protecciones otorgadas en los dos primeros requisitos del Principio de Proporcionalidad.

En segundo lugar, la orden debe describir los objetos por registrar o capturar con "especificidad". El requisito de especificidad prohíbe llevar a cabo registros generales y asegura que el registro tendrá limitaciones temporales y de alcance.[29] La necesidad de especificidad se asemeja bastante al cuarto requisito del Principio de Proporcionalidad—que establece que la "información a la que se accederá estará limitada a lo relevante y material".

Estos principios de la Cuarta Enmienda se han puesto a prueba—y se han extendido—al aplicarlos a los nuevos métodos de vigilancia, como los simuladores de torres de telefonía (también conocidos como "Recolectores IMSI", "IMSI catchers" o "StingRays"), así como la vigilancia de las comunicaciones que rastrea grandes cantidades de datos sobre comunicaciones, como los programas de vigilancia masiva de la NSA o los "vertederos de información extraída de torres de telefonía" (*tower dump)* llevados a cabo por los órganos de aplicación de la ley. Hasta el momento, la Corte Suprema no se ha referido a las implicaciones de la Cuarta Enmienda en relación con estas nuevas formas de vigilancia de las comunicaciones, lo que deja a los tribunales federales en la lucha inicial en contra de estas

cuestiones. Los simuladores de torres de telefonía se relacionan con los intereses de "razonabilidad" de la Cuarta Enmienda—tanto por la gran cantidad de información recolectada como por la sensibilidad de la información de ubicación obtenida por el uso de estos aparatos.[30] Progresivamente, los tribunales federales inferiores han mostrado poca predisposición para aprobar el uso de simuladores de torres de telefonía sin contar con una orden basada en una sospecha fundada.[31] En vista de esta creciente reticencia, el Ministerio de Justicia de Estados Unidos anunció recientemente que se requerirá de las agencias federales de aplicación de la ley la obtención de una orden antes de la implementación de simuladores de torres de telefonía.[32]

Incluso antes de que sucedieran estos cambios, muchas cortes supremas estatales ya ofrecían más claridad—y mayor protección constitucional—para la información de ubicación obtenida mediante el teléfono celular de una persona. Por ejemplo, la Corte Suprema de Florida (el tribunal superior estatal de Florida) determinó que el uso de información extraída de torres de telefonía en tiempo real por parte de la policía sin contar con una orden representa una violación a la Cuarta Enmienda.[33] Análogamente, la Corte Suprema de Nueva Jersey determinó que, bajo la Constitución estatal del estado de Nueva Jersey, el acceso a la información histórica de una torre de telefonía sin tener una orden queda prohibido.[34]

Otras referencias de la Cuarta Enmienda se relacionan con los "vertederos de información mediante torres de telefonía"—la obtención de registros de todos los teléfonos celulares que se conectan con una torre específica obtenidos por órganos de aplicación de la ley. Algunos jueces federales concluyeron que los intentos de las agencias de la aplicación de la ley para obtener acceso a los registros de conexión de las torres de telefonía representan una violación a la Cuarta Enmienda.[35] Al menos un juez concluyó que los vertederos de información de las torres de telefonía (*tower dump, en inglés*) constituyen "registro[s] generalizado[s] e invasivo[s] que afecta[n] posiblemente a cientos de personas" que requieren, como mínimo, una orden basada en una sospecha fundada.[36]

De hecho, algunos jueces reconocieron que los vertederos de información extraída de torres de telefonía (*tower dumps*) y los simuladores de torres (*IMSI catchers*) son tan intrusivos que sólo debería emitirse una orden que contenga protecciones adicionales para la privacidad—protecciones destinadas a salvaguardar la privacidad de los inocentes cuyos datos son extraídos durante el proceso de vigilancia.[37] Estas preocupaciones reflejan el quinto requisito del Principio de Proporcionalidad en relación con la retención de "información excedente" y su pronta destrucción o devolución.

Finalmente, al abordar las cuestiones relativas a la vigilancia masiva de los registros de

llamadas de los estadounidenses, al menos un juez federal llegó a la conclusión de que el programa de la Agencia de Seguridad Nacional no pudo cumplir con los requisitos adaptados de la Cuarta Enmienda. El juez notó que:

> *[El programa de vigilancia de registro de llamadas de la NSA] no es, como cuestión preliminar, una incursión discreta o específica. Por el contrario, es un programa demasiado general y verdaderamente pasmoso, dirigido a millones de estadounidenses de manera arbitraria e indiscriminada.*

La incapacidad de aplicar criterios discriminatorios o de adaptar la vigilancia—en otras palabras, la falta de Proporcionalidad—resulta en la inconstitucionalidad del programa, a los ojos de este juez.[38]

Protecciones Jurídicas

Los valores incorporados en el Principio de Proporcionalidad también están expresados—y con mayor alcance que aquel que le da la Constitución—en la legislación a nivel federal y estatal.

Una de las primeras leyes que regula la vigilancia de las comunicaciones en Estados Unidos —la Ley de Escuchas—codifica muchos de los valores consagrados en el Principio de Proporcionalidad, y superpone procedimientos adicionales más allá de la sospecha fundada requerida por la Constitución federal. Entre otras cosas, la ley de Escuchas exige que los funcionarios del gobierno demuestren que (1) investigan una serie de delitos graves y específicos; (2) existe una sospecha probable para creer que la vigilancia proveerá comunicaciones acerca de ese delito grave; y (3) otros métodos más normales y menos intrusivos no pudieron o no podrían cumplir el objetivo, entre otros requisitos.[39]

No obstante, la Ley de Escuchas no regula la totalidad de la vigilancia de las comunicaciones en Estados Unidos. Por ejemplo, otro conjunto de leyes regula la vigilancia en el contexto de la seguridad nacional;[40] y la Ley de Escuchas, junto con sus últimas reformas, sólo aplica a la interceptación en "tiempo real" de los contenidos de las comunicaciones, lo que deja una protección estatutaria diferente a nivel federal en cuanto a las comunicaciones "almacenadas", como los e-mails, o la información relativa a una comunicación, como la información de ubicación o los metadatos.[41]

En vista de estas deficiencias, varios estados han aprobado leyes que brindan mayor protección para los ciudadanos y que añaden restricciones a la vigilancia de las comunicaciones. Una vez más, como se describió anteriormente, el hito legislativo de California del 2015 ahora exige que la policía obtenga una orden para poder tener acceso a la

información de ubicación de una persona y a otras formas de metadatos asociados con las comunicaciones electrónicas. Otros estados—como Utah[42] Virginia,[43] y Minnesota[44]—aprobaron leyes que exigen una orden previa al acceso de las agencias de aplicación de la ley a la información de ubicación.

B. Áreas de la legislación de EE. UU. que requieren desarrollar con más profundidad el Principio de Proporcionalidad

Pese a las protecciones descriptas más arriba, el Principio de Proporcionalidad no se ajusta uniformemente a la totalidad de la legislación de EE. UU. Las violaciones del Principio se dan con frecuencia en la vigilancia destinada a los "metadatos" de las comunicaciones—como la práctica de la NSA de recolectar los registros de llamados de forma masiva o los intentos de los órganos de aplicación de la ley para extraer datos del "volcado de información de torres de telefonía" (*tower dumps*). Si bien algunas cortes, como las mencionadas anteriormente, están empezando a reconocer la sensibilidad de la recolección de los metadatos—especialmente la recolección en masa—estas cortes siguen siendo la minoría. La mayoría de las cortes todavía opina que la recolección de metadatos—incluso de manera masiva—no es merecedora de protección constitucional. Las teorías jurídicas que motivan la recolección masiva de metadatos explotan el nivel desigual de las protecciones brindadas para los "contenidos" y los "metadatos" de las comunicaciones bajo la legislación de EE. UU. Bajo el precedente establecido en la Corte Suprema desde los años setenta, descripto más arriba, los individuos no tienen intereses relacionados con la Cuarta Enmienda en la recolección de al menos una determinada cantidad de registros almacenados por terceros.[45] Sin embargo, a raíz de tal precedente, algunas cortes han llegado a la conclusión errónea de que puede que nunca exista un interés en los metadatos de las comunicaciones reconocido constitucionalmente. El Tribunal de Vigilancia de Inteligencia Extranjera (tribunal FISC) sostuvo, en una decisión en defensa de la constitucionalidad del programa de recolección de registros de llamadas de la NSA, que:

> *Si un individuo no tiene un interés relacionado con la Cuarta Enmienda, agrupar un gran número de individuos que estén en la misma situación no dará como resultado un interés relacionado con la Cuarta Enmienda que surja de la nada, ex nihilo.*[46]

Tal conclusión evidentemente viola el Principio de Proporcionalidad. De hecho, el "agrupar" la información de "un gran número" de personas altera fundamentalmente la sensibilidad de los datos: lo que, de manera aislada, puede no ser muy revelador se transforma radicalmente en el proceso de "agrupación". Las decisiones como estas se alejan del requisito fundamental de "razonabilidad" de la Cuarta Enmienda y, por eso, violan el

Principio de Proporcionalidad.

En Estados Unidos, la ausencia de Proporcionalidad no se limita a la vigilancia relativa a los metadatos. Por ejemplo, la NSA examina el contenido de grandes cantidades de tráfico internacional de Internet, en busca de direcciones de correos electrónicos u otros datos que identifiquen a las personas de interés.[47] La denominada "sobre la vigilancia" ["about" surveillance] se lleva a cabo sin órdenes judiciales o autorizaciones particularizadas emitidas por un tribunal y da lugar al registro del tráfico de Internet de millones de inocentes, ciudadanos en los que no se encuentra focalizada la investigación.

Una vez más, es primordial el apego más estricto a la piedra de toque de la Cuarta Enmienda —la "razonabilidad", ya que no daría lugar a este tipo de vigilancia, que es arrasadora y generalizadora y que claramente carece de Proporcionalidad.

IV.
Recomendaciones

- Las cortes deberían exigir que las opiniones que autoricen nuevas técnicas de vigilancia o que planteen nuevas preguntas sobre la legislación y la tecnología estén disponibles al público tan pronto como sea posible. Si la divulgación de cierta opinión fuera imposible por razones de seguridad nacional o cuestiones de aplicación de la ley, debería redactarse y publicarse un resumen cuidadoso que informe al público sobre la naturaleza de la disputa legal y sobre las conclusiones de la corte.
- Al usar la amplia reforma de vigilancia de California como modelo, las reformas federales o estatales no deberían crear distinciones arbitrarias entre los tipos de información protegida, como las distinciones actuales que existen entre "contenido" y "metadatos", o comunicaciones "almacenadas" y en "tiempo real". El acceso a la información protegida debe basarse en una orden emitida por un juez imparcial a raíz de una sospecha fundada.
- Dicha reforma debe incluir también la protección de los datos de ubicación, como la información recolectada a través de simuladores de torres de telefonía, y asegurar que tales datos no sean obtenidos sin una orden basada en una sospecha fundada emitida por un juez imparcial.
- Las cortes deberían reconocer y reforzar el requisito fundamental de "razonabilidad" de la Cuarta Enmienda y prohibir así los intentos del gobierno de recolectar y analizar información protegida de manera masiva o cualquier otra forma que elimine definitivamente la habilidad de mantener una comunicación privada.

1 https://necessaryandproportionate.org/

2 Sentencia sobre The Sunday Times v. Reino Unido, expediente Nº 6538/74, Sentencia del 26 de abril de 1979, párr .49.

3 Siver v. Reino Unido, Petra v. Rumania, 1998. La Comisión de Derechos Humanos adopta el mismo enfoque. Observación General No. 34, CCPR/C/GC/34, 12 de septiembre de 2011, párrs. 24 – 26, disponible en http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f34&Lang=en

4 Kyllo v. Estados Unidos, 533 EE. UU. 27, 33 (2001); Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); Estados Unidos v. Jones, 132 S. Ct. 945, 949 (2012).

5 Pruneyard Shopping Center v. Robins, 447 EE. UU. 74, 81 (1980) ("[El gobierno federal no] limita el poder del Estado para ejercer su facultad policial o su derecho de soberanía con el fin de adoptar en su propia Constitución libertades individuales más abarcativas que aquellas conferidas por la Constitución [f]ederal"). Véase, en general, O'Connor v. Johnson, 287 N.W.2d 400, 405 (Minnesota, 1979) ("Los estados pueden, como lo reconoce en varias ocasiones la Corte Suprema de los Estados Unidos, brindarles a sus ciudadanos mayor protección que las garantías provistas en la Constitución Federal. En efecto, los Estados son 'responsables de manera independiente de salvaguardar los derechos de sus ciudadanos'").

6 Estados Unidos v. Robinson, 414 EE. UU. 218, 234-35 (1973).

7 Compárese Estados Unidos v. Flores-López, 670 F.3d 803, 805-10 (7ma instancia 2012) (la policía puede registrar un teléfono celular para obtener el número de línea conducente a arresto); El Pueblo v. Diaz, 51 Cal.4º 84, 101, 244 P.3d 501, 511 (2011) (idem) con Smallwood v. el Estado, 113 So.3º 724, 738 (Florida, 2013); el Estado v. Smith, 124 Calle Ohio. 3º 163, 171, 920 N.E.2º 949, 956 (2009) (la policía no está habilitada a registrar un teléfono celular conducente a arresto).

8 Smith v. Maryland, 442 EE. UU. 735 (1979).

9 Estados Unidos v. Jones, 132 S.Ct. 945, 957 (2012) (Jueza Sotomayor, opinión concurrente).

10 Commonwealth v. Augustine, 4 N.E.3d 846 (Massachussetts, 2014); El Estado v. Earls, 70 A.3d 630 (Nueva Jersey, 2013); Tracey v. State, 152 So.3d 504 (Florida, 2014).

11 18 U.S.C. 2703(a).

12 *Véase* 18 U.S.C. 2703(b), (c).

13 Los tribunales federales también han implementado mayores protecciones, más allá de las provistas por la ECPA. Por ejemplo, el Tribunal de Apelaciones del Sexto Circuito, durante una sentencia influyente, determinó que la Cuarta Enmienda protege a los e-mails en posesión de terceros (los proveedores), sin prejuicio de la duración de su almacenamiento. *Estados Unidos v. Warshack*, 631 F.3d 266 (6º Cir. 2010).

14 Leyes Revisadas de Hawaii. 803-47.6; 16 M.R.S.A. § 642; Código Procesal Penal de Texas 18.21; Código de Utah Comentado. § 77-23b-4(a).

15 Véase Leyes Revisadas de Colorado con Comentarios. § 16-3-303.5(2); 16 Leyes Revisadas de Maine con Comentarios. § 648; Leyes Revisadas de Minnesota con Comentarios. §§ 626A.28(3)(d), 626A.42(2); Código de Montana Comentado. § 46-5-110(1)(a); Código de Utah Comentado. § 77-23c-102(1)(a). Seis estados han aprobado

leyes que exigen a la policía obtener una orden de registro para rastrear un teléfono celular en tiempo real. Véase, Código de Indiana. § 35-33-5-12; Leyes de Wisconsin con Comentarios. § 968.373(2); 725 ILCS 168/10; Código de Maryland, Procesal Penal 1-203.1; Código de Virginia Comentado. 19.2-56.2; HB 1440, que modificó el Nuevo Código de Washington 9.73.260 el 11 de mayo de 2015.

16 https://www.eff.org/deeplinks/2015/10/victory-california-gov-brown-signs-calecpa-requiring-police-get-warrant-accessing

17 *Véase, por ejemplo*, *Papachristou v. Jacksonville*, 405 EE. UU. 156, 162 (1972) ("Vivir bajo un estado de derecho conlleva varias suposiciones, una de las cuales es que '(todas las personas) tienen el derecho de que se les informe sobre lo que el Estado dispone o prohíbe'"); *Bancos v. Manchester*, 128 EE. UU. 244, 253 (1888) (Los dictámenes judiciales representan "la auténtica exposición e interpretación de la ley, la que, siendo obligatoria para todos los ciudadanos, [es] de libre publicación para todos[.]"); *Sheppard v. Maxwell*, 384 EE. UU. 333, 349 (1966) ("El principio de que la justicia no puede sobrevivir detrás de los muros del silencio se refleja desde hace mucho tiempo en la 'desconfianza angloamericana hacia los juicios secretos'").

18 *Véase* Orden Ejecutiva 13526 (que regula la clasificación de la información sobre seguridad nacional).

19 *Véase* la Ley de Vigilancia de Inteligencia Extranjera [Foreign Intelligence Surveillance Act] de 1978, 50 U.S.C. § 1801 *y subsiguientes* (que crean el FISC [Tribunal de vigilancia de inteligencia extranjera] y exigen órdenes judiciales para la vigilancia de inteligencia extranjera).

20 *Véase* Walter F. Mondale, Robert A. Stein, Caitlinrose Fisher, *Ya no hay un juez imparcial: El tribunal de vigilancia de inteligencia extranjera como consecuencia de la guerra contra el terrorismo*, 14, 34 (1 de enero de 2016), Boletín Jurídico Minnesota Law Review, próxima edición (en la que se toma nota de que el tribunal FISC se ha convertido más en un "sello de goma" que en un control de extralimitaciones del poder ejecutivo).

21 La ley también autoriza al gobierno a brindar un resumen desclasificado de cualquier decisión importante que haya tomado el tribunal FISC, cuando la desclasificación de la propia sentencia resulte imposible.

22 Esta técnica, conocida como construcción paralela de la prueba, se utiliza para evitar que los acusados en causas penales tomen conocimiento de que una técnica de vigilancia específica fue implementada en el caso. Esto, a su vez, aísla el uso de la técnica y las órdenes que le dieron lugar a partir de la impugnación jurídica. *Véase, por ejemplo*, John Shiffman & Kristina Cooke, *Agentes directos de EE. UU. encubren programa utilizado para investigar a estadounidenses*, Reuters, *disponible en* http://www.reuters.com/article/us-deasod-idUSBRE97409R20130805

23 Un "Objetivo Legítimo", a los efectos de los principios corresponde a un interés jurídico preponderante e importante que es necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición. *Véase* https://en.necessaryandproportionate.org/ ("Objetivo Legítimo").

24 Los 13 Principios definen a la información protegida como toda "información que incluye, refleja, surge de, o se refiere a las comunicaciones de una persona y que no está fácilmente disponible y accesible para el público en general. Tradicionalmente, el carácter invasivo de la Vigilancia de las Comunicaciones ha sido evaluado sobre la base de categorías artificiales y formalistas. Los marcos legales existentes distinguen entre "contenido" o "no contenido", "información del suscriptor" o "metadatos", datos almacenados o datos en tránsito, datos que se tienen en el hogar o en la posesión de un tercero proveedor de servicios.7 Sin embargo, estas distinciones ya no son apropiadas para medir el grado de intromisión que la Vigilancia de las Comunicaciones realiza en la vida privada y las relaciones de las personas. Aunque desde hace tiempo se ha acordado que el contenido de la comunicación merece una protección significativa en la ley debido a su capacidad de revelar información sensible, ahora está claro

que existe otra información que surge de las comunicaciones, y datos que no son contenido, que puede revelar incluso más acerca de una persona que el contenido en sí, y por lo tanto merece una protección equivalente. Hoy en día, cada uno de estos tipos de información, por sí sola o analizada colectivamente, puede revelar la identidad de una persona, su comportamiento, sus asociaciones, sus condiciones físicas o estado de salud, su raza, color, orientación sexual, origen nacional o puntos de vista, o puede permitir el mapeo de la ubicación de la persona, sus movimientos e interacciones en el tiempo,8 o puede hacer esto respecto de todas las personas en una ubicación determinada, incluyendo una manifestación pública u otro acontecimiento político. Como resultado, toda la Información Protegida debe recibir la máxima protección de la ley".

25 Ohio v. Robinette, 519 EE. UU. 33 (1996).

26 Katz v. Estados Unidos, 389 EE. UU. 347, 353 (1967).

27 Illinois v. Gates, 462 EE. UU. 213, 232 (1983).

28 Id.

29 Estados Unidos v. Berger, 388 EE. UU. 41, 56 (1967) (que deja sin efecto el estatuto sobre escuchas careciente de especificidad ya que "la necesidad de especificidad[. . .]es particularmente importante en el caso de las escuchas").

30 Estados Unidos v. En materia de la petición de Estados Unidos, 15-M-0021 (W.D. Ill. 2015) at 7.

31 *Véase, por ejemplo,* En materia de la petición de los Estados Unidos de América sobre una orden que autorice la instalación y el uso de aparatos de registro, captura y rastreo de comunicaciones, 2012 WL 2120492 (S.D. Texas. 2012).

32 *Véase* El ministerio de justicia anuncia mejoras en las políticas sobre simuladores de torres de telefonía (septiembre de 2015), *disponible en* http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.

33 Tracy v. Florida, 11-224 (Florida S. Ct. 2014). Si bien no quedó claro si la policía utilizó un simulador de torre de telefonía para la obtención en tiempo real de información sobre ubicación en este caso, la posesión aplicaría en una situación semejante.

34 Nueva Jersey v. Earls, 70 A.3d 630 (Nueva Jersey 2013).

35 En el caso de la petición de EE. UU. de una orden que autorice la publicación de información histórica de torre de telefonía, 809 Suplemento Federal 2d 113, 126 (E.D.N.Y. 2011) ("El advenimiento de la tecnología de recolección de registros de ubicación mediante torres de telefonía dio paso a la vigilancia constante sobre una gran parte de la población estadounidense: un nivel de intromisión gubernamental sin precedentes").

36 En lo que respecta a Estados Unidos ex rel. Orden, según la sección 18 U.S.C. 2703(d), 930 Suplemento Federal 2d 698 (S.D. Texas. 2012).

37 *Véase* id. 702 ("Si bien el uso de vertederos de información (tower dump) a través de torres de telefonía aprobado por la corte termina inevitablemente en manos del Gobierno, para recibir tales datos, el Gobierno debería al menos adoptar un protocolo para abordar el manejo de información privada sensible".); *véase también* Estados Unidos v. En materia de la petición de Estados Unidos, *supra* 27 ("[L]a Corte piensa que el proceso debe establecerse para asegurar razonablemente que la información de terceros inocentes recolectada a través del uso de simuladores de torres de telefonía no quede retenida por Estados Unidos o cualquier órgano del gobierno".)

38 Klayman v. NSA, 957 Suplemento Federal 2d 1 (D.D.C. Noviembre 2015).

39 18 U.S.C. § 2518(3).

40 *Véase, en general,* la Ley de Vigilancia de Inteligencia Extranjera [the Foreign Intelligence Surveillance Act], codificada en 50 U.S.C. ch. 36.

41 La Ley de Comunicaciones Almacenadas [The Stored Communications Act], 18 U.S.C. §§ 2701-27012.

42 http://le.utah.gov/~2014/bills/static/HB0128.html

43 https://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+HB1408ER

44 https://www.revisor.mn.gov/statutes/?id=626A.42

45 Smith v. Maryland, 442 EE. UU. 735 (1979).

46 https://fas.org/irp/agency/doj/fisa/fisc-082913.pdf.

47 *Véase, por ejemplo*, Junta de Supervisión de Privacidad y Libertades Civiles, *Informe sobre el programa de vigilancia operado de acuerdo con la sección 702 de la Ley de Vigilancia de Inteligencia Extranjera*, 7, 35-37 (2 de julio de 2014) (el cual describe la vigilancia en la infraestructura troncal y la vigilancia sobre terceros ["about" surveillance]).