Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú

Por Miguel Morachimo
con los aportes de Katitza Rodríguez

Julio 2016

ELECTRONIC FRONTIER FOUNDATION

hiperderecho

Miguel Morachimo es abogado por la Pontificia Universidad Católica del Perú, Director de la ONG Hiperderecho.

Informe preparado en alianza con la Electronic Frontier Foundation (EFF). Agradecemos los aportes de Katitza Rodríguez, Directora Internacional de Derechos Humanos por la revisión sustantiva del informe, Kim Carlson y David Bogado de EFF por la corrección de estilo y formato.

El presente reporte forma parte del proyecto regional "Vigilancia y Derechos Humanos" llevado a cabo en ocho países de América Latina por la Electronic Frontier Foundation, una organización internacional sin fines de lucro que desde 1990 defiende la libertad de expresión y la privacidad en el entorno digital.

Hiperderecho es una organización civil peruana sin fines de lucro dedicada a facilitar el entendimiento público, investigar y promover el respeto de los derechos y libertades en entornos digitales.

Índice de contenido

Introducción

Pocos asuntos como la vigilancia estatal de las comunicaciones han despertado una gran polémica internacional en los últimos años. Muchas sospechas se confirmaron en junio del año 2013 cuando Edward Snowden, un ex contratista del gobierno de los Estados Unidos de América, reveló a la prensa internacional pruebas contundentes sobre la existencia de distintos programas nacionales e internacionales dirigidos por la Agencia Nacional de Seguridad (NSA) de Estados Unidos y destinados a vigilar en forma masiva las comunicaciones privadas de millones de usuarios de Internet.

Desde entonces, no sólo en Estados Unidos sino también en el resto del mundo se ha abierto un debate público sobre el contexto y los límites en los que resulta válido que un estado monitoree sistemáticamente a sus ciudadanos con la finalidad de preveer o reducir la comisión de delitos y realizar labores de inteligencia. Este debate enfrenta, de un lado, a quienes creen que estas medidas resultan necesarias en tanto son el precio para contrarrestar un mal mayor como actos de violencia y terrorismo. Del otro lado, están quienes se oponen a este tipo de medidas porque creen que entregar al estado el completo control sobre las comunicaciones de sus nacionales constituye una violación incontestable de los derechos fundamentales y debilita las instituciones democráticas.

La polémica en torno a la vigilancia no sólo resulta relevante para los gobiernos y el proceso democrático sino también para los usuarios y las empresas privadas. Una encuesta realizada a finales del 2013 por el Centro PEN International encontró que el 24% de los escritores encuestados había evitado deliberadamente abordar ciertos temas por teléfono o correo electrónico, mientras que otro 9% había considerado seriamente empezar a hacerlo, como consecuencia de las actividades de vigilancia denunciadas por la prensa internacional.[1] Adicionalmente, se estima que la relación entre algunas de las principales empresas tecnológicas de Estados Unidos y los programas de vigilancia de la NSA podrían llegar a traducirse en pérdidas de hasta un 25% de las ganancias anuales del sector, debido a la potencial pérdida de confianza de los consumidores y socios comerciales.[2]

Perú ha tenido una historia compleja de vigilancia estatal y privada. Durante los años de 1990 al 2001, se registraron múltiples casos y denuncias por vigilancia e intervención de las comunicaciones a cargo del desaparecido Servicio Nacional de Inteligencia. Desde entonces, se sospecha que los especialistas y equipos destinados para este fin no han desaparecido sino que en algunos casos han pasado al sector privado y en otros casos han sido repotenciados u orientados hacia otros objetivos. En el 2011, la investigación del periodista Óscar Castilla dio a conocer el funcionamiento de un sistema de intervención de las comunicaciones operado por la División Antidrogas de la Policía Nacional. Este sistema cuenta, con equipos y la

asistencia técnica de la Drug Enforcement Administration (DEA) de Estados Unidos, que había empezado a operar desde el 2009 para casos de narcotráfico y crimen organizado.[3]

Durante las primeras semanas del 2015, se publicaron en los medios de comunicación distintas denuncias sobre operaciones de inteligencia llevadas a cabo por la Dirección de Inteligencia Nacional (DINI) con fines políticos o estratégicos para el gobierno. A consecuencia de estas revelaciones, en febrero de 2015 la Presidencia del Consejo de Ministros anunció su decisión de disolver la DINI y replantear todo el esquema de inteligencia nacional. Un mes después estas mismas revelaciones motivaron una exitosa moción de censura contra todo el gabinete ministerial presidido por Ana Jara, la primera censura en más de 52 años en Perú.[4]

En julio de 2015 se publicó una nueva norma, popularmente conocida como #LeyStalker, que amplia los poderes de la Policía para acceder, sin orden judicial, a la ubicación de cualquier usuario de telecomunicaciones en tiempo real y en caso de flagrante delito, así como, se instauró un mandato obligatorio de retención de datos por 3 años. Recientemente, en septiembre del 2015, un nuevo proyecto de ley busca derogar la norma anterior, y en su lugar establece un régimen legal de colaboración entre Policía Nacional, Ministerio Público y Poder Judicial de cara a la obtención de los datos de geolocalización de cualquier dispositivo móvil.[5]

En este contexto, resulta relevante trasladar el debate sobre la vigilancia a otros entornos y realidades. Las justificaciones legales y herramientas tecnológicas que hacen posible estas prácticas en ciertos estados pueden rápidamente ser traspasadas e implementadas a través de las empresas privadas que prestan diferentes servicios de telecomunicaciones en nuestro país. La urgencia de estudiar las nuevas formas de vigilancia estatal y revisar las leyes nacionales que regulan estas prácticas a la luz de los estándares internacionales de derechos humanos ha sido reconocida por el Relator Especial para la Libertad de Expresión de las Naciones Unidas, en su reporte de abril de 2013.[6] Desde esa perspectiva, este reporte desarrolla el contenido y los alcances de las distintas formas de vigilancia llevadas a cabo por el Estado Peruano y su relación con los derechos fundamentales. Su finalidad es analizar si los distintos mecanismos y justificaciones existentes para los mecanismos de vigilancia estatal en Perú resulten respetuosos de los límites que impone el derecho constitucional, según están reconocidos en el Derecho Peruano y han sido interpretados por tribunales nacionales y extranjeros.

En la primera sección se aproxima un concepto de actividad de Vigilancia de las Comunicaciones según ha sido definida por la jurisprudencia internacional. A continuación, se discute cómo las actividades de vigilancia pueden entrar en conflicto con el contenido esencial de ciertos derechos fundamentales, conforme están reconocidos en la Constitución, sus normas de desarrollo y en la jurisprudencia del Tribunal Constitucional.

En la tercera sección se listan las distintas formas de Vigilancia de las Comunicaciones que permite el marco legal peruano y se analiza su pertinencia respecto de los estándares internacionales en materia de derechos humanos que sirven de límite a la vigilancia de las comunicaciones Estatal. Finalmente, se formulan recomendaciones de política pública concretas que pueden servir de base para futuras reformas legislativas.

I.
¿De Qué Hablamos Cuando Hablamos de Vigilancia Estatal de las Comunicaciones?

Las comunicaciones y la esfera privada de un individuo resultaban algo relativamente sencillo de identificar y resguardar en un mundo analógico. Las únicas copias de las comunicaciones privadas residían en manos de sus destinatarios y cualquier dato relacionado con la vida privada de una persona solo podía llegar tan lejos como llegaba la credibilidad del interlocutor. Si una persona no quería que algún aspecto de su vida personal llegase a conocimiento de terceros o del público en general le bastaba con cerrar bien su puerta. Por ello, ni la preocupación ni la noción jurídica de privacidad se materializaron hasta la invención de tecnologías como la fotografía.

Es precisamente a propósito de la creciente práctica de publicación de fotografías en periódicos y revistas que este concepto es esbozado en los Estados Unidos en el seminal artículo *The Right to Privacy* de Samuel Warren y Louis Brandeis a fines del siglo XIX. De hecho, en su artículo, los autores mencionan específicamente el problema de que la prensa pueda sobrepasar los umbrales de la vida privada gracias a la proliferación de las cámaras fotográficas.[7]

En el pasado, la invención de la fotografía los teléfonos nos llevaron a plantearnos por primera vez la necesidad de identificar y proteger legalmente nuestra privacidad. Los límites para la intervención de estos medios de comunicación se encontraban asentados en principios legales claros y en restricciones físicas del propio medio (ej., era imposible vigilar una llamada telefónica sin acceder físicamente a la red en algún punto). En los años recientes, el uso de aparatos permanentemente conectados a Internet y la evolución hacia la "Internet de las cosas" nos exige replantear los límites de lo que entendemos o no como protegido frente a la Vigilancia Estatal de las Comunicaciones y de la información privada.

Hoy en día una fotografía sacada con un *teléfono inteligente* tiene implicancias radicalmente distintas de las que tenía la misma fotografía hecha con una cámara analógica. En principio, desde una fotografía digital pueden realizarse innumerables copias idénticas en forma inmediata y a costos insignificantes. Además, la fotografía puede contener información adicional o *metadatos* como la hora, la fecha, el modelo de la cámara, las coordenadas geográficas del lugar en el que fue tomada e incluso el nombre del autor o el número de serie de la cámara que se usó. Adicionalmente, cuando las fotografías digitales se realizan con *smartphones* o *tablets* existe una buena posibilidad de que una copia de la

misma sea inmediata e incluso automáticamente alojada en un servidor externo del proveedor del dispositivo, del proveedor de servicios de Internet, o de un tercer proveedor de servicios de almacenamiento remoto (por ejemplo, Apple, Google o Dropbox, respectivamente). Estos nuevos escenarios hacen muy relevante la discusión sobre el tratamiento legal de la privacidad y la pertinencia de las herramientas legales con las que contamos para prevenir su vulneración, particularmente de parte de la autoridad.

De la misma manera, las nuevas tecnologías, la proliferación de servicios permanentemente conectados a un servidor y la capacidad de procesamiento de información a través de bases de datos, exigen replantear la protección del derecho a la privacidad a otros espacios que tradicionalmente no estaban protegidos. Así, por ejemplo, antes una lista con los números de teléfono con los que se comunicó un teléfono celular durante un periodo determinado de horas o días significaba poco en términos de vulneración a la vida privada. Actualmente, las empresas operadoras de telecomunicaciones tienen en su poder registros que incluyen frecuencia, lugar, hora y duración de cada comunicación que abarcan varios años y que les permite el procesamiento de información de tal manera que pueden obtener datos y hábitos de la vida privada de una persona que resultan reveladores de su intimidad, como son los lugares en los que pasa la noche o los números a los que llama con más frecuencia.

I.1. Actividades de Vigilancia Estatal de las Comunicaciones

Este reporte considera dentro del término "vigilancia estatal" cualquier medida justificada o no que pueda tomar una autoridad nacional con la finalidad de acceder a cualquier tipo de información relacionada con el desarrollo o el contenido de las comunicaciones privadas de una persona a través de cualquier medio de monitoreo, interceptación, recolección, preservación y retención de las mismas. Resulta indiferente el medio a través del cual se lleve a cabo el proceso de vigilancia, el cual puede realizarse en forma manual con intervención humana o mecánica mediante acceso y almacenamiento automático de la información. De la misma manera, este concepto se utiliza con independencia de que haya mediado o no una justificación legal o una autorización expresa o tácita de cualquier tipo. Este reporte reconoce que existen formas válidas y legales de vigilancia de las comunicaciones por la autoridad y sus límites son discutidos con detalle en las siguientes secciones.

La experiencia internacional señala que el ejercicio de actividades de vigilancia estatal de las comunicaciones no necesariamente se desarrolla en el marco de programas gubernamentales específicos reconocidos como tales. En ocasiones, la vigilancia estatal de las comunicaciones puede presentarse en la forma de mecanismos aislados de monitoreo, registro o intervención de comunicaciones por parte de distintos servicios o autoridades, ya sea como parte de las actividades de los sistemas de administración de justicia o de inteligencia.

Según su alcance, la vigilancia estatal de las comunicaciones puede llevarse a cabo de manera

individualizada o de forma masiva. En el primer supuesto, se entiende que se lleva a cabo de manera individualizada o dirigida cuando está orientada hacia un individuo o grupo de sujetos en particular (ej. investigados por la comisión de un delito). Por el contrario, se considera masiva cuando la vigilancia se ejerce respecto de un grupo amplio de personas que no necesariamente se encuentran conectadas con una investigación concreta o son parte de un proceso (ej. interceptar las llamadas de todos los miembros de un partido político o de vecinos de una zona geográfica concreta).

A su vez, las actividades de vigilancia pueden llevarse a cabo a través de una amplia gama de medidas técnicas, incluyendo: la escucha telefónica, la intervención de las comunicaciones electrónicas, la difusión de programas de ordenador maliciosos (*malware, spyware*) o el control remoto de teléfonos celulares o computadoras con la finalidad de extraer información del vigilado. También existen, técnicas de vigilancia masiva como el monitoreo de datos de comunicaciones o *metadatos* desde las fibras ópticas de acceso a internet, el acceso a los datos de geolocalización de un usuario, la retención obligatoria de datos, entre otros. Las diversas herramientas tecnológicas a través de las cuales se llevan a cabo las actividades de vigilancia estatal son objeto de constante evolución y estudio.

Finalmente, la vigilancia estatal de las comunicaciones también incluye las obligaciones impuestas legalmente o a través de órdenes particulares de una autoridad a terceros como empresas de telefónicas o prestadores de servicios de Internet de registrar el desarrollo o el contenido de las comunicaciones de los usuarios y entregar dichos registros a la autoridad. Bajo este supuesto, la vigilancia estatal de las comunicaciones no es ejercida en forma directa por el Estado sino en forma indirecta a través del acceso a las comunicaciones e información protegida de los usuarios almacenados o bajo el control de terceros.

No se incluyen en esta definición los casos en los que la vigilancia se lleva a cabo en forma independiente sin mediar obligación legal u orden de autoridad, por parte de terceros individuos o empresas (ej. espionaje empresarial). Estos casos de intervención privada de las comunicaciones constituyen igualmente una acción ilegal según las leyes peruanas, en tanto no hayan sido autorizados por el usuario del servicio, y pueden ser investigadas y sancionadas penalmente. Sin embargo, dado que no media intervención del Estado en la actividad de vigilancia estatal, su análisis estará fuera del ámbito de este reporte.

I.2. Información Protegida

Tradicionalmente se entendía como 'información protegida' exclusivamente al contenido mismo de una comunicación, como las conversaciones telefónicas o el contenido de una carta. Sin embargo, las nuevas formas y medios de comunicación interpersonal con los que contamos actualmente nos obligan a ampliar el ámbito de lo que entendemos como información protegida susceptible de vigilancia para incluir otros elementos como los

registros geográficos asociados a la comunicación, la información identificadora de los terminales utilizados, entre otros, que permite a través de su procesamiento obtener información acerca del comportamiento del agente de dichas comunicaciones.

En esos términos, este reporte considera como información que puede ser objeto de los programas de vigilancia por parte del Estado a cualquier información relacionada con el proceso de comunicación de una persona o grupo de personas, siempre que no haya sido hecha pública previamente. Esta definición incluye no sólo el contenido mismo de las comunicaciones sino también otros elementos relacionados con el desarrollo de la comunicación, tales como su oportunidad, frecuencia, ruta, origen y destino. Ello, en concordancia con el criterio establecido por la Corte Interamericana de Derechos Humanos, la cual ha señalado que la definición elegida no sólo alcanza al contenido mismo de las comunicaciones sino también cualquier otra información accesoria al contenido mismo como "cualquier otro elemento del proceso de comunicación".[8]

En sede nacional, nuestro Tribunal Constitucional ha hecho suyas las conclusiones del caso *Escher v. Brasil* en su sentencia recaída sobre el Expediente No. 00655-2010-PHC/TC al precisar que el derecho a la vida privada tutela "a las conversaciones telefónicas independientemente de su contenido e incluso puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones".[9]

En el caso específico de la actividad de comunicación a través de Internet, la definición de información protegida alcanza también a elementos como los datos asociados al número IP, los historiales de navegación, y toda aquella información recogida por aplicaciones de seguimiento de las actividades en Internet, tales como las *cookies*, entre otros.

II.
¿Qué Derechos Fundamentales se Ven Amenazados por la Vigilancia Estatal de las Comunicaciones?

Conforme han sido definidas en la sección anterior, las actividades de vigilancia por la autoridad pueden constituir una amenaza para el ejercicio de diversos derechos como la libertad de expresión y la privacidad según están definidos por la Constitución y los tratados internacionales de derechos humanos de los que Perú es parte. Esta sección describe la tensión existente entre las distintas modalidades de vigilancia estatal de las comunicaciones y los derechos fundamentales señalados.

Esto no significa que toda forma de vigilancia estatal de las comunicaciones sea ilegal y deba estar proscrita en un estado de derecho. Específicamente, la valoración de cómo y bajo qué garantías es posible ejercer la vigilancia estatal en una forma proporcional y compatible con el respeto de los derechos humanos será presentada al final de esta misma sección.

II.1. ¿Cómo Afecta la Vigilancia Estatal de las Comunicaciones a la Privacidad?

El primer derecho que se ve comprometido en el marco de las actividades de vigilancia estatal de las comunicaciones es el derecho a la privacidad. Este comprende el derecho de toda persona a que la información relacionada con su intimidad personal y familiar no sea objeto de acceso, registro o alteración por parte de terceros sin que medie autorización. Por ende, cuando el Estado lleva a cabo actividades destinadas a registrar, interferir o acceder en las comunicaciones y registros electrónicos de una persona está inmiscuyéndose en la esfera de la intimidad personal o familiar del sujeto.

La Declaración Universal de Derechos Humanos señala en su artículo 12 que nadie puede ser objeto de injerencias arbitrarias en su vida privada ni en su familia, su domicilio o su correspondencia y señala que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.[10] En correspondencia, el derecho a la privacidad también se encuentra reconocido en los artículos 11 de la Convención Americana sobre Derechos Humanos[11] y 17 del Pacto Internacional de Derechos Civiles y Políticos.[12]

En nuestro país, dicho derecho se encuentra amparado en el artículo 2 de la Constitución

Política de 1993 que en varios numerales señala el derecho de todos los ciudadanos a: (i) que los servicios informáticos no suministren informaciones que afecten la intimidad personal y familiar, (ii) a la intimidad personal y familiar, (iii) a la inviolabilidad del domicilio, y (iv) al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.

En esa línea, el Tribunal Constitucional peruano ha reconocido en repetida jurisprudencia los alcances de este derecho, que entiende como:

"[...] el ámbito personal en el cual un ser humano tiene la capacidad de desarrollar y fomentar libremente su personalidad. Por ende, se considera que está constituida por los datos, hechos o situaciones desconocidos para la comunidad que, siendo verídicos, están reservados al conocimiento del sujeto mismo y de un grupo reducido de personas, y cuya divulgación o conocimiento por otros trae aparejado algún daño."[13]

Por ende, se entiende que la protección de la privacidad no está circunscrita a espacios geográficos u objetos en particular sino que, en general, abarca a cualquier espacio, objeto o situación desde la cual se puedan conocer hechos que están reservados al conocimiento del sujeto mismo o de un grupo reducido de personas y cuya difusión puede significar un daño a la persona.

Sobre la privacidad de las comunicaciones, la propia Constitución peruana establece en su artículo 2 que "Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley". En el mismo sentido, el artículo 4 del Texto Único Ordenado de la Ley de Telecomunicaciones señala que toda persona tiene derecho a la inviolabilidad y al secreto de las telecomunicaciones,[14] mientras que el artículo 13 de su Reglamento precisa que se atenta contra la inviolabilidad y el secreto de las telecomunicaciones cuando deliberadamente una persona que no es quien origina ni es el destinatario de la comunicación, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, divulga, utiliza, trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación sin la autorización de quienes están involucrados en la comunicación.[15]

Finalmente, otra salvaguarda legal de la privacidad la encontramos en la Ley de Protección de Datos Personales cuando se señala en su artículo 13:

"Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los datos personales obtenidos con violación de este precepto

carecen de efecto legal".[16]

Según las disposiciones legales citadas, cualquier captura o intervención de las comunicaciones potencialmente constituye una afectación al derecho a la privacidad. Sobre este punto, el Consejo de Derechos Humanos de Naciones Unidas ha precisado que en algunos casos la mera posibilidad de interferencia o recolección de esta información ya constituye una afectación a la privacidad.[17]

II.2. ¿Cómo Afecta la Libertad de Expresión la Vigilancia Estatal de las Comunicaciones?

Conforme lo señala el artículo 2 de la Constitución peruana, la libertad de expresión conlleva el derecho de toda persona a la libertad de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento alguno. En correspondencia, la Declaración Universal de Derechos Humanos reconoce en su artículo 19 que este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.[18] Así también lo definen el artículo 13 de la Convención Americana sobre Derechos Humanos[19] y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos.[20]

En esa misma línea, el Tribunal Constitucional peruano ha entendido este derecho fundamental como la garantía de que "las personas (individual o colectivamente consideradas) puedan transmitir y difundir libremente ideas, pensamientos, juicios de valor u opiniones".[21]

La actividad de vigilancia estatal de las comunicaciones también tiene la capacidad de afectar la libertad de expresión, en tanto bajo situaciones de vigilancia muchos individuos pueden verse castigados por el contenido de sus comunicaciones o autocensura las mismas con la finalidad de no ser objeto de represión. Las consecuencias perniciosas de la vigilancia estatal de las comunicaciones y la auto censura han sido investigadas en un amplio número de experimentos de ciencia social y demuestran cómo esto no solo afecta el activismo social y político sino que cambia fundamentalmente hasta los comportamientos más domésticos.[22]

En términos simples, los individuos tienden a comportarse de manera distinta cuando saben que están siendo observados y ello incide negativamente sobre sus libertades para decir, opinar y recibir información de cualquier tipo. Esto aplica no sólo para quienes ejercen estos derechos para el activismo social y político sino que incluso se puede verificar entre quienes usan las herramientas de comunicación para fines domésticos o educacionales.

En contextos de vigilancia estatal de las comunicaciones que afecta el grado de privacidad y resulta en consecuencia, una condicionante del ejercicio del derecho a la libertad de expresión. Así lo ha señalado el Relator Especial de Naciones Unidas, para quien la privacidad y la libre expresión están vinculadas y resultan mutuamente dependientes.[23]

II.3. Un Modelo de Compatibilidad Entre Vigilancia Estatal de las Comunicaciones y Respeto de los Derechos Fundamentales

Desde que se observó la forma en que las actividades de vigilancia estatal pueden comprometer el ejercicio de los derechos fundamentales se ha estudiado y discutido largamente dónde deben trazarse los límites. La mejor fuente para responder esta interrogante reside en los distintos tratados internacionales suscritos por los estados. La validez de sus preceptos para responder esta cuestión ha sido confirmada en sede nacional también por el propio Tribunal Constitucional peruano al señalar:

"Como todo derecho fundamental, la vida privada no es un derecho absoluto, por lo que puede ser restringido siempre que las injerencias no sean abusivas o arbitrarias; esto es, que tales injerencias deben encontrarse previstas en la ley, perseguir un fin legítimo y ser idóneas, necesarias y proporcionales en una sociedad democrática (artículo 11.2 de la Convención Americana sobre Derechos Humanos). Semejante situación sucede con el derecho al secreto y a la inviolabilidad de las comunicaciones."[24]

En respuesta a esta pregunta, en diciembre de 2013 la Asamblea General de Naciones Unidas emitió su Resolución 68/167 sobre el derecho a la privacidad en la era digital.[25] En dicha Resolución, la Asamblea exhorta a los estados a respetar el derecho a la privacidad en entornos digitales a través de una evaluación de procedimientos, prácticas y legislación de vigilancia con miras a afianzar el derecho a la privacidad, cuidándose de cumplir sus obligaciones en virtud del derecho internacional de los derechos humanos. También señala que deben de establecerse mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia estatal de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado.

A solicitud de la Asamblea General, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos presentó en junio de 2014 al Consejo de Derechos Humanos y a la Asamblea General un detallado informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales. Este informe señala expresamente que para responder las preguntas sobre dónde colocar los límites a la vigilancia estatal es necesario discutir lo que se debe entender por injerencias "arbitrarias" o "ilegales" en la vida privada. Concluye que las prácticas de vigilancia resulten

aceptables en el derecho internacional deberán de ser: (i) previstas expresamente en la ley, (ii) necesarias para alcanzar un fin legítimo, (iii) proporcionales en los términos del objetivo trazado, y, (iv) proporcionen salvaguardas efectivas contra el uso indebido.

Desde la sociedad civil internacional, un esfuerzo reciente y valioso por sistematizar el contenido de las distintas fuentes de Derecho Internacional y utilizarlas para establecer límites a las actividades de vigilancia estatal de las comunicaciones son los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[26] Este documento desarrollado y escrito colaborativamente por organizaciones civiles dedicadas a la protección de la privacidad y abogados de derechos humanos de todo el mundo bajo el liderazgo de Electronic Frontier Foundation, Access y Privacy International, propone una lista de trece principios que interpretan derechos contenidos en tratados internacionales que buscan ser una fórmula para determinar si cierta actividad de vigilancia estatal resulta lícita en el marco del sistema internacional de protección de los derechos humanos.

En tanto los tratados y decisiones que interpretan los principios son también aplicables a nuestro país, el estándar propuesto por los mencionados Principios resulta una fuente de doctrina relevante y útil para analizar las prácticas de vigilancia por las autoridades locales. Este documento señala que en toda actividad de vigilancia estatal de las comunicaciones se debe de respetar los siguientes principios:

i. ***legalidad***, según el cual toda limitación a los derechos humanos debe ser prescrita expresamente por una norma de rango legal de conocimiento públic;

ii. ***objetivo legítimo***, que señala que sólo se deberá de permitir la vigilancia estatal cuando corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática;

iii. ***necesidad***, por el que los sistemas de vigilancia estatal deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo;

iv. ***idoneidad***, que señala que cualquier caso de vigilancia de las comunicaciones autorizada mediante ley debe ser apropiada para cumplir el objetivo legítimo específico identificado;

v. ***proporcionalidad***, que indica que el ejercicio de la vigilancia de las comunicaciones estatal debe acreditar que se respeta en la mayor medida posible los derechos humanos afectados por la medida implementada;

vi. ***autoridad judicial competente***, según el cual las decisiones relacionadas con la vigilancia de las comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente;

vii. ***debido proceso***, que plantea la necesidad de reconocer el derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley,

viii. ***notificación al usuario***, según el cual la autoridad debe de notificar a aquellos cuyas comunicaciones están siendo vigiladas con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización, en la medida en la que ello no afecte la finalidad perseguida;

ix. ***transparencia***, conforme al cual los Estados deben ser transparentes publicando información sobre el uso y alcance de las leyes de vigilancia de las comunicaciones, reglamentos, actividades, poderes o autoridades implicadas en su ejercicio;

x. ***supervisión pública***, señala que los Estados deben establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones;

xi. **integridad de las comunicaciones y sistemas**, según el cual los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de vigilancia de las comunicaciones;

xii. ***garantías para la cooperación internacional***, conforme al cual los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la vigilancia de las comunicaciones, se adopte el estándar disponible con el mayor nivel de protección para las personas; y,

xiii. ***garantías contra el acceso ilegítimo y el derecho al recurso*** efectivo, según el cual los Estados deben promulgar leyes que penalicen la vigilancia de las comunicaciones ilegal por parte de actores públicos o privados, así como proveer sanciones penales y civiles suficientes y adecuadas, protección a los *informantes* y medios de reparación a las personas afectadas.

III.
Prácticas de Vigilancia Estatal de las Comunicaciones

Esta sección del reporte describe las prácticas de vigilancia estatal legalmente reconocidas por el marco jurídico nacional y evalúa su idoneidad respecto del marco internacional de derechos humanos en los términos de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones arriba reseñados.

III.1. Vigilancia Estatal de las Comunicaciones en el Ambito del Sistema Penal

La legislación penal vigente en nuestro país regula en dos grupos normativos la vigilancia de las comunicaciones: (i) en las normas que establecen los procedimientos aplicables para la intervención de las comunicaciones de las personas como medio de recopilación de medios probatorios en una investigación penal; y, (ii) a través de los tipos penales que califican como delito la vigilancia ilegal de las comunicaciones.

Por un lado, la forma más frecuente de vigilancia de las comunicaciones se lleva a cabo en el marco de una *investigación penal*: (i) a través de las medidas de interceptación e incautación postal, y, (ii) mediante las que ordenan la intervención de comunicaciones y telecomunicaciones. El procedimiento general aplicable a cualquier tipo de intervención de las comunicaciones está descrito en la Ley 27.697 y detallado en los códigos Penal y Procesal Penal, así como en el Protocolo de Actuación Conjunta para la Intervención o Grabación de Registro de comunicaciones Telefónicas o de Otras Formas de Comunicación, aprobado por Resolución Ministerial No. 0243-2014-JUS.

Conforme a este marco legal, solo un juez puede autorizar a un fiscal hacer uso de la facultad de conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional y solo puede hacerlo respecto de una lista particular de delitos que abarca los de: (i) secuestro, (ii) trata de personas, (iii) pornografía infantil, (iv) robo agravado, (v) extorsión, (vi) tráfico ilícito de drogas, (vii) tráfico ilícito de migrantes, (viii) delitos contra la humanidad, (ix) atentados contra la seguridad nacional y traición a la patria, (x) peculado, (xi) corrupción de funcionarios, (xii) terrorismo, (xiii) delitos tributarios y aduaneros, (xiv) lavado de activos; y, (xv) delitos informáticos.

El procedimiento de intervención de las comunicaciones solo puede ser solicitado por los Fiscales Penales, los Procuradores Públicos y el Fiscal de la Nación, en los casos de su competencia. La actividad de vigilancia estatal de las comunicaciones es ejecutada por el personal autorizado del Ministerio Público y/o de la Policía Nacional del Perú bajo supervisión del fiscal a cargo de la investigación. Para ello, la ley señala que pueden contar con el apoyo técnico de las empresas operadoras de comunicaciones con la finalidad de asegurar la intervención o control de las mismas en tiempo real y, si las características de las comunicaciones lo requieren, también puede solicitar el apoyo de personas naturales o jurídicas expertas en la actividad de recolección.

Se distinguen dos etapas en la intervención de las comunicaciones: la recolección y el control. En la primera se alude a los procesos mediante los cuales se recoge o registra la comunicación, mientras que la segunda comprende la toma de conocimiento oficial del contenido de la comunicación y la eliminación de las partes que no revisten interés para la investigación.

La solicitud que envíe el fiscal al juez debe de estar sustentada y contener todos los datos necesarios. Además, debe de incluir específicamente los elementos indiciarios que permitan al juez emitir bajo su criterio la respectiva autorización. Si la solicitud es denegada, el fiscal puede apelar al superior jerárquico desde el día siguiente de enterado o notificado. El pedido del fiscal y la autorización judicial deben de contener las especificaciones que sean necesarias para distinguir las distintas clases de recolección y de control que pretende llevarse a cabo, incluyendo:

i. Si la comunicación es una determinada; si se va a dar probablemente dentro de un conjunto indeterminado de comunicaciones; o si es una comunicación cierta que sucederá dentro de circunstancias determinadas.

ii. Si la comunicación se dará en el futuro o ya se dio en el pasado.

iii. Si la comunicación es accesible a toda persona que la perciba, a ella o su medio, o si se encuentra cerrada o cifrada.

iv. Si se han hecho uso de medios destinados a encubrir la identidad del emisor o del receptor de la comunicación, o de cualquier otra persona, hecho o circunstancia que se mencionan en la comunicación; así como la puesta de cualquier dificultad destinada a impedir el acceso o la identificación de la comunicación, de sus partes, o de la información en ella mencionada.

Durante el periodo de recolección autorizado, el fiscal podrá ir haciendo controles de modo periódico, sobre lo que se haya recolectado a la fecha, si es que el modo de recolección fuese

compatible con esa metodología. Si durante este periodo se descubren indicios de otros hechos delictivos, el fiscal deberá de comunicarlo al juez competente para que disponga la pertinencia o no de su utilización en la investigación en curso (en vía de ampliación) o para que el Ministerio Publico determine si hay merito para iniciar la investigación penal sobre el tema descubierto.

Finalmente, la propia Ley 27.697 señala que todos los involucrados en el proceso de investigación (el juez, el personal del juzgado, el fiscal, su personal de apoyo, la Policía Nacional del Perú, peritos, Procuradores Públicos y demás personas naturales o jurídicas autorizadas) deberán guardar reserva sobre toda la información que obtengan como resultado de la intervención de las comunicaciones. El incumplimiento de esta obligación de confidencialidad, se señala, se sanciona con inhabilitación sin perjuicio de las responsabilidad penales, civiles y administrativas aplicables.

En noviembre de 2014 se aprobó el Protocolo de Intervención o Grabación de Registro de Comunicaciones, mediante Resolución Ministerial No. 0243-2014-JUS, que buscar ordenar el procedimiento en etapas más claras para su mejor implementación por parte de la Policía Nacional, el Ministerio Público y el Poder Judicial. Este Protocolo divide el procedimiento en siete etapas y detalla sus requisitos: (i) informe policial inicial determinando la necesidad de la medida, (ii) solicitud o requerimiento fiscal, (iii) resolución judicial, (iv) notificación de la resolución al fiscal, (v) ejecución de la medida, (vi) transcripción de las grabaciones, (vii) control o reexamen a pedido del afectado.

III.1.1. Intervención de Comunicaciones Postales con Fines de Investigación y Prevención

El artículo 226 del Código Procesal Penal regula el procedimiento de intervención de comunicaciones postales como cartas, pliegos, valores, telegramas y otros objetos de correspondencia o envío postal. Este solo puede darse a pedido del fiscal y por autorización del Juez de la Investigación Preparatoria. El Código requiere que la orden judicial se expida cuando su obtención sea indispensable para el debido esclarecimiento de los hechos investigados y podrá prolongarse por el tiempo estrictamente necesario, el que no será mayor que el período de la investigación. La intervención postal no puede abarcar un periodo mayor que el de la investigación del caso.

Sobre la notificación al sujeto de la vigilancia, el artículo 227 señala que cuando se haya cumplido con la diligencia y se hayan realizado las investigaciones inmediatas se deberá de poner en conocimiento del afectado todo lo actuado, quien puede instar el reexamen judicial, dentro del plazo de tres días de notificado. En dicha audiencia, el juez decidirá si la diligencia se realizó correctamente y si la interceptación e incautación han comprendido comunicaciones relacionadas con la investigación.

III.1.2. Intervención de Comunicaciones Telefónicas o Similares (Incluyendo Electrónicas) con Fines de Investigación y Prevención

El artículo 230 del Código Procesal Penal señala que cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad el fiscal podrá solicitar al juez de la investigación preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación del investigado o personas relacionadas a él.

Sin embargo, el propio artículo establece la limitación de que debe de acreditarse que la intervención resulta absolutamente necesaria para proseguir las investigaciones. Para ello, se precisa que el requerimiento y la resolución judicial que autoriza la vigilancia deberá de indicar el nombre y dirección del afectado por la medida si se conociera, así como la identidad del teléfono u otro medio de comunicación o telecomunicación a intervenir, grabar o registrar, forma de la interceptación, su alcance y su duración, dependencia policial o Fiscalía que se encargará de la diligencia de intervención y grabación o registro. Se establece que la interceptación o actividad de vigilancia no puede durar más de sesenta (60) días naturales, aunque excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del fiscal y decisión motivada del juez de la investigación preparatoria. Cuando los elementos de convicción tenidos en consideración para ordenar la medida desaparecen o haya vencido el plazo solicitado para llevar a cabo la interceptación deberá de interrumpirse inmediatamente.

De la misma manera, el artículo 231 del Código Procesal Penal señala que deberán de ser registradas mediante la grabación y aseguramiento de la fidelidad de la misma. Adicionalmente, dispone que las grabaciones, indicios y/o evidencias recolectadas durante el desarrollo de la ejecución de la medida dispuesta por mandato judicial y el Acta de Recolección y Control serán entregados al fiscal, quien es el encargado de su conservación con todas las medidas de seguridad al alcance y quien debe de cuidar que las mismas no sean conocidas por personas ajenas al procedimiento.

Sobre la notificación y posibilidad de impugnación de la medida, el citado artículo 231 del Código Procesal Penal señala que una vez ejecutada la medida de intervención y realizadas las investigaciones inmediatas en relación al resultado de aquélla, se deberá de poner en conocimiento del afectado todo lo actuado, quien puede instar el reexamen judicial, dentro del plazo de tres días de notificado. Sobre el particular, el Código precisa que la notificación al afectado sólo será posible si el objeto de la investigación lo permitiere y en tanto no pusiere en peligro la vida o la integridad corporal de terceras personas. Finalmente, se establece que el secreto de las actividades de vigilancia practicadas requerirá resolución judicial especial motivada y estará sujeta a un plazo que el juez deberá de fijar.

En forma accesoria a este procedimiento, el Código Procesal Penal reconoce en el artículo 231

un mecanismo de emergencia exclusivamente aplicable cuando se toma conocimiento de nuevos sujetos o números telefónicos que necesitan intervenirse para prevenir delitos de terrorismo, tráfico ilícito de drogas y secuestro a cometerse en un breve periodo de tiempo. En estos casos, la intervención podrá ser dispuesta directamente por el fiscal con cargo a que posteriormente se notifique al juez para su convalidación.

Por su parte, el artículo 207 del Código Procesal Penal señala que en las investigaciones por delitos violentos, graves o contra organizaciones delictivas, el fiscal, por propia iniciativa o a pedido de la policía, y sin conocimiento del afectado, puede ordenar llevar a cabo acciones de vigilancia sobre un sujeto a través de tomas fotográficas y cualquier otro medio técnico especial de observación. Sin embargo, el propio artículo 207 señala que sólo se requerirá de autorización judicial cuando los medios técnicos de investigación se realicen en el interior de inmuebles o lugares cerrados.

III.1.3. Uso de Dispositivos de Vigilancia Estatal de las Comunicaciones para la Restricción de la Libertad Individual

El artículo 52 del Código Penal establece otro caso en el que la autoridad puede someter a vigilancia electrónica a un sujeto. Así, señala que un juez puede, de oficio o a petición de parte, convertir la pena privativa de libertad en pena de vigilancia electrónica personal. Esta facultad está desarrollada en la Ley 29.499, que entiende a la vigilancia electrónica personal un mecanismo de control que tiene por finalidad monitorear el tránsito tanto de procesados como de condenados, dentro de un radio de acción y desplazamiento, teniendo como punto de referencia el domicilio o lugar que señalen, usando como mecanismo de control brazaletes, tobilleras o dispositivos corporales.

III.1.4. Protección de las Comunicaciones Contra Actividades de Vigilancia Estatal

En otro grupo de disposiciones, el Código Penal sanciona en diversos artículos una serie delitos que pueden cometer los privados cuando llevan a cabo actividades de vigilancia, como los de violación de la intimidad personal y familiar (artículo 154), tráfico de datos personales (artículo 154-A), revelación de la intimidad personal y familiar (artículo 156), uso indebido de archivos computarizados (artículo 157), violación del secreto de las comunicaciones (artículo 161), interferencia telefónica (artículo 162), supresión o extravía indebido de correspondencia (artículo 163), y, publicación indebida de correspondencia (artículo 164).

III.2. Vigilancia en el Ambito del Sistema de Inteligencia

El Sistema de Inteligencia Nacional también contempla situaciones en las que se puede recurrir a la vigilancia de las comunicaciones, según los procedimientos descritos en el

Decreto Legislativo 1141 sobre el Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia – DINI y su reglamento.[27]

El artículo 32 del Decreto Legislativo 1141 regula los procedimientos especiales de obtención de información, que define como aquellos que se utilizan para acceder a información que resulta estrictamente indispensable para el cumplimiento de los objetivos de la actividad de inteligencia y cuya realización es aprobada por cualquiera de los dos (02) Jueces Superiores Ad hoc del Poder Judicial designados por la Corte Suprema de Justicia de la República especialmente para este fin.

El artículo 33 del mencionado Decreto Legislativo señala que la autorización para la ejecución de un procedimiento de este tipo deberá de ser solicitada únicamente por el Director de Inteligencia Nacional, y deberá contener: (i) la identificación de la persona o personas que serán afectadas; (ii) la especificación de las medidas que se solicitan; y, (iii) motivación y duración de las medidas solicitadas.

En el mismo artículo se precisa que la resolución judicial que emite el Juez Superior Ad hoc se tramita dentro de las veinticuatro (24) horas de presentada la solicitud. La resolución judicial tiene carácter vinculante para todas las entidades públicas que deben coadyuvar a su realización, debiendo observar las disposiciones sobre información clasificada. Si la realización del procedimiento es denegada, procede recurso de apelación, el que será resuelto por una Sala Superior Ad hoc presidida por el otro Juez Superior Ad hoc y los dos Jueces Superiores Ad hoc suplentes, que también se debe de tramitar y resolver en un plazo de veinticuatro (24) horas.

Estableciendo un procedimiento paralelo, el mismo Decreto Legislativo 1141 señala que en caso de peligro contra la seguridad nacional y por la urgencia de las circunstancias, el Director de Inteligencia Nacional podrá, excepcionalmente, autorizar la ejecución de un procedimiento especial de obtención de información. La autorización de ejecución debe realizarse con cargo a formalizar la solicitud de inmediato ante el Juez Superior Ad hoc, quien en plazo de veinticuatro (24) horas puede convalidarlo o disponer su inmediata paralización. Así mismo, precisa que ante mandato de paralización, procede recurso de apelación.

La propia norma citada establece que en ningún caso los informes de inteligencia tendrán valor probatorio dentro de procesos judiciales, administrativos y/o disciplinarios, pero su contenido podrá constituir elemento orientador durante la investigación. En ese sentido, el artículo 35 obliga a que toda información obtenida para la producción de inteligencia por el Sistema de Inteligencia Nacional (SINA) que resulte innecesaria para el objetivo del sistema por corresponder a la esfera de su vida privada debe ser destruida por los funcionarios

responsables de los componentes del sistema que la detecte, bajo responsabilidad de inhabilitación y sin perjuicio de las sanciones civiles y/o penales que correspondan.

Sobre la posibilidad de control externo de las actividades de vigilancia en el marco del sistema de inteligencia, el artículo 5 del Decreto Legislativo 1141 señala que en uso de sus funciones de control y fiscalización, las autoridades, funcionarios o instituciones autorizados por ley, pueden solicitar el acceso a información clasificada de inteligencia a los componentes del SINA, la que será proporcionada con obligatorio conocimiento de la Dirección Nacional de Inteligencia. Según su diseño actual, formulado por el Decreto Legislativo 1141, la Dirección Nacional de Inteligencia está sujeta a tres espacios de control:

> ***Poder Judicial:*** Cuando necesita acceder a información que se encuentra protegida por el secreto de las telecomunicaciones o el secreto bancario. En estos casos, existen dos jueces superiores especialmente nombrados por la Corte Suprema que trabajan exclusivamente recibiendo y respondiendo las solicitudes de "obtención de información" que formula la Dirección de Inteligencia.
>
> ***Poder Legislativo:*** La Comisión de Inteligencia del Congreso es lo más cercano que existe a una autoridad independiente capaz de revisar todas las acciones de inteligencia. Incluso tiene potestad de revisar todos los planes de inteligencia, los expedientes tramitados ante los Jueces que atienden las solicitudes de obtención de información y recibe un informe anual directamente del Director de Inteligencia.
>
> ***Contraloría:*** El Órgano de Control Institucional solo tiene potestad para supervisar las actividades de gestión administrativa, económica y financiera de los recursos y bienes de los componentes del Sistema de Inteligencia Nacional

III.3. Vigilancia a Cargo de la Policía Nacional

Desde finales de julio de 2015 está vigente en Perú una nueva norma que permite a la Policía acceder a los datos de geolocalización en tiempo real de cualquier usuario de celulares o de dispositivos electrónicos conectados a una red de telecomunicaciones. El Decreto Legislativo No. 1182 busca regular el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación en la lucha contra la delincuencia y el crimen organizado por parte de la Policía Nacional.

Este Decreto Legislativo crea un mecanismo mediante el cual la policía puede enviar un pedido a cualquier empresa operadora para acceder a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos. Según la norma, tras la solicitud de la Policía, empresas de telecomunicaciones tales como Movistar o Claro están inmediatamente obligadas a proporcionar acceso en tiempo real a esta información. Para

lograrlo, la policía no necesita obtener ningún tipo de autorización judicial previa que autorice la compartición de esta información.

Según la propia norma, la policía solo podrá utilizar este mecanismo cuando concurran tres requisitos en simultáneo: (i) se trate de un delito flagrante,[28] (ii) el delito investigado sea sancionado con pena superior a los cuatro años de cárcel, y, (iii) el acceso a esta información constituya un medio necesario para la investigación. El cumplimiento de estos requisitos solo será revisado luego de que la policía ya haya accedido a los datos. Así, la unidad a cargo de la investigación policial tendrá veinticuatro (24) horas para enviar al fiscal un informe que sustente su requerimiento y el fiscal tendrá otras veinticuatro (24) horas para solicitar a un juez la "convalidación de la medida". A su vez, el juez que reciba el pedido tendrá otras 24 horas para pronunciarse sobre la legalidad del pedido y establecer un periodo durante la cual estará vigente.

Bajo este sistema, podrían pasar hasta 72 horas desde que la Policía empezó a monitorear a cualquier ciudadano para que recién un juez pueda pronunciarse sobre la legalidad de la medida y verifique si realmente se han respetado los requisitos.

Según el esquema anteriormente vigente, si la Policía necesitaba acceder a la geolocalización de cualquier línea telefónica era necesario que sea un fiscal quien se lo solicite a un juez, se trate o no de un delito flagrante. Resultaba responsabilidad del fiscal convencer al juez que existían indicios suficientes como para amparar esta solicitud y era el magistrado quien establecía la forma, oportunidad, periodo y garantías aplicables a la intervención.

Desde la entrada en vigencia de este nuevo Decreto, la información que antes la policía solo podía obtener mediante una autorización judicial expresa, ahora podrá obtenerla directamente de las empresas de comunicaciones a su solo pedido si es que consideran que están inmersos dentro de los supuestos de hecho establecidos por el Decreto Legislativo No. 1182.

En su artículo 6, el referido Decreto Legislativo precisa que este mecanismo solo podrá aplicar a los datos de geolocalización de los usuarios de servicios públicos de telecomunicaciones y, por tanto, queda fuera del ámbito de aplicación de esta norma cualquier tipo de intervención de las telecomunicaciones que deberán regirse por procedimientos especiales. Además, el artículo 7 señala un régimen de responsabilidad para quienes en su calidad de agentes de la policía usen maliciosamente este sistema y, a su vez, establece que los operadores y sus dependientes deben de guardar reserva respecto de la información facilitada a la policía bajo este mecanismo.

A principios de Septiembre del 2015, se presentó el Proyecto de Ley No. 4809/2015-CR firmado por el congresista Héctor Becerril y otros cinco congresistas de la bancada Fuerza

Popular, el cual busca derogar el Decreto Legislativo 1182.[29] La propuesta es un ejercicio de reescritura del citado decreto conservando en buena medida muchos de sus artículos pero con un cambio fundamental: el acceso a los datos de localización o geolocalización solo puede ser autorizado por el Juez Penal de turno. Los tres supuestos concurrentes en los que este pedido puede realizarse se mantienen: (i) flagrancia delictiva, (ii) pena mayor a cuatro años, y, (iii) juicio de necesidad. En su artículo 4, el Proyecto señala que todo el procedimiento desde que el Ministerio Público hace el pedido hasta que el Juez Penal lo autoriza o rechaza debería de durar máximo veinticuatro (24) horas y promueve que la comunicación se lleve a cabo a través de teléfono, correo electrónico, teleconferencia o cualquier otro medio.

La propuesta también buscar restituir al Fiscal como conductor de la investigación del delito. Según el Decreto Legislativo No. 1182, la Policía era la única que podía solicitar el acceso inmediato a los datos de geolocalización. Para el Proyecto de Ley, esto significaba un desconocimiento del rol constitucional del Ministerio Público como encargado principal de la investigación de cualquier delito desde su inicio.

Por eso, en su artículo 3 propone que sea el Ministerio Público el único autorizado para solicitar con carácter de urgencia al Juez Penal de turno el acceso a los datos de localización o geolocalización. De esta manera, la propuesta también sería consistente en el Código Procesal Penal que autoriza al Fiscal hacer lo propio durante la Investigación Preparatoria. Por ende, el mecanismo de la ley permitiría formular estas solicitudes y acceder a esta información durante las diligencias preliminares previas a la investigación preparatoria.[30]

En octubre de 2015, mediante Resolución Ministerial No. 0631-2015-IN, el Ministerio del Interior aprobó el "Protocolo de acceso a los datos de golocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar", que establece las etapas del procedimiento de acceso a la información de geolocalización creado por el Decreto Legislativo No. 1182. Sin embargo, amparándose en la excepción de seguridad nacional de la Ley de Transparencia y Acceso a la Información Pública, el Ministerio ha considerado al texto mismo del Protocolo como de carácter "reservado". Esto significa que ningún ciudadano peruano puede conocer el contenido o tener acceso al texto de este protocolo, pese a que el procedimiento en él descrito puede resultar de aplicación para cualquier usuario de servicios públicos de telecomunicaciones en Perú. Luego de pocos meses de aprobado este Protocolo, un representante del Ministerio del Interior señaló en una entrevista periodística que entre diciembre de 2015 y enero de 2016 se habían registrado 45 solicitudes de geolocalización aunque no precisó en cuántos casos se había logrado detener a los sospechosos.[31]

III.4. Deber de Colaboración de las Empresas de Telecomunicaciones en las Actividades de Vigilancia estatal de las Comunicaciones

La ley peruana también establece deberes de colaboración para las empresas privadas como parte de las Actividades de Vigilancia estatal. La principal obligación que contempla la legislación peruana es la de retención de datos de tráfico relacionados con las comunicaciones que está desarrollada en el Decreto Legislativo No. 1182, vigente desde julio de 2015.[32]

Así, en la Segunda Disposición Complementaria Final del referido Decreto se obliga a todos los concesionarios de servicios públicos de telecomunicaciones (telefonía fija, celular y acceso a Internet) y a las entidades públicas relacionadas con estos servicios a conservar los "datos derivados de las telecomunicaciones" por un periodo de hasta treinta y seis (36) meses o tres años. Al respecto, se precisa que los datos correspondientes a los primeros doce (12) meses deberán de ser almacenados en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real a las autoridades después de recibida la autorización judicial.

Complementariamente, los datos de los veinticuatro (24) meses adicionales deberán de ser guardados en un sistema de almacenamiento electrónico especial y entregados dentro de los siete (7) días siguientes a la autorización judicial. Según lo establecido por el propio Decreto Legislativo, el incumplimiento de estas obligaciones acarreará responsabilidad por parte de las empresas operadoras. Sin embargo, dada la reciente promulgación de esta nueva obligación todavía no queda claro qué datos quedarán comprendidos como "datos derivados de las telecomunicaciones". Aunque se entienden que esta obligación de conservación de datos no podrá afectar el contenido mismo de las comunicaciones, la reglamentación pendiente de la norma podría incluir o excluir ciertas clases de metadatos.

Hasta antes del Decreto Legislativo No. 1182, existía exclusivamente la obligación de conversar la información posible de ser supervisada por el organismo regulador y la información de tráfico de llamadas por hasta dos (2) meses. Sin embargo, con la entrada en vigencia del referido Decreto Legislativo estas normas no han sido derogadas.

Por un lado, la Ley No. 27.336 señala que las entidades bajo supervisión del Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) tienen la obligación de conservar por un período de al menos 3 (tres) años después de originada la información bajo supervisión del regulador incluyendo la tasación, los registros fuentes del detalle de las llamadas y facturación de los servicios que explota y aquellas que tenga que conservar para cumplir con normas técnicas declaradas de observancia obligatoria en el país por una autoridad competente, o con obligaciones contractuales o legales aplicables a dichos servicios.[33] Por otro lado, una obligación similar de conservación de registros aunque mucho

más reducida la encontramos en las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, la norma de derechos de los usuarios aprobada por OSIPTEL. Específicamente, el artículo 65 de las Condiciones de Uso señala que los abonados tienen el derecho de solicitar a las empresas operadoras una copia de su registro de información de llamadas entrantes de hasta dos (2) meses anteriores.[34] En correspondencia, ello implica que las empresas operadoras están obligadas a conservar la información de llamadas entrantes y salientes de sus abonados durante al menos dos (2) meses para cumplir con esta obligación.

Además, el citado artículo 230 del Código Procesal Penal también señala que los concesionarios de servicios públicos de telecomunicaciones están obligados a facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento.

Adicionalmente, señalan que los trabajadores de dichas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento. El propio artículo establece la obligación legal de los concesionarios de otorgar acceso, compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. En el mismo sentido, se precisa que cuando por razones de innovación tecnológica los concesionarios renueven sus equipos y software, se encontrarán obligados a mantener la compatibilidad con el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú.

En el caso especial de las tareas de control de comunicaciones del sistema de inteligencia, el artículo 41 del Decreto Legislativo 1141 señala que toda persona natural o jurídica está obligada legalmente a contribuir con el Sistema de Inteligencia Nacional (SINA) brindando obligatoriamente y en forma gratuita la información que sea requerida por el ente rector del sistema, vinculada a las labores de inteligencia. El mismo artículo establece que en caso que la información solicitada esté amparada por algún deber de reserva, la entrega de tal información no constituirá una violación a dicho deber, toda vez que la misma continuará bajo este principio, al cual se encuentra obligado todo el personal de inteligencia. La única excepción que se plantea a esta obligación es cuando se compromete información protegida por el secreto profesional, intimidad personal y familiar, secreto bancario, reserva tributaria y otras reconocidas por la Constitución.

III.5. ¿Respeta la Legislación Peruana Los Estándares Internacionales en Materia de Actividades de Vigilancia Estatal?

La legislación nacional reseñada en esta sección nos presenta una visión panorámica de

cómo el Estado Peruano entiende y utiliza la vigilancia de las comunicaciones en casos de delito flagrante. A propósito de las reformas penales y de inteligencia que se llevaron a cabo en los últimos años, la mayoría de estas normas tienen menos de diez años de vigencia y todavía siguen siendo modificadas. En esta etapa, llama la atención en especial la diferencia que existe en la provisión de salvaguardas para los derechos fundamentales entre los sistemas penales y de inteligencia.

En términos de *legalidad*, se aprecia que los límites y requisitos de la intervención de las comunicaciones en el marco de una investigación penal están mucho mejor delimitados que las que se realizan bajo el sistema de inteligencia. Por un lado, bajo el sistema penal se señala todo lo que puede ser objeto de vigilancia y se exige que aquello resulte expresamente comprendido dentro de la solicitud y posterior autorización, mientras que bajo el sistema de inteligencia sólo se alude a "medidas de obtención de información" sin detallar cuáles pueden resultar comprendidas.

Incluso en el sistema penal falta precisión en el alcance que debe de tener la vigilancia para los casos en los que se intervienen comunicaciones o dispositivos electrónicos. Están mucho más desarrollados los criterios a utilizarse en los casos de intervención de comunicaciones telefónicas pero hay pocos elementos orientadores para la intervención de otro tipo de comunicaciones a través de Internet como cuentas de correo electrónico o perfiles en redes sociales. Mención aparte merece el mecanismo de acceso a la información sobre geolocalización. Una seria violación al principio de legalidad es la decisión del Ministerio de declarar como "reservado" el Protocolo que señala el procedimiento de acceso a datos de geolocalización de usuarios de teléfonos móviles y dispositivos electrónicos. A través de esta decisión, el gobierno peruano ha creado una "ley secreta" que aunque se podrá aplicar a cualquier ciudadano peruano ninguno de los potenciales afectados podrá conocerla. Esta decisión es también contradictoria respecto de decisiones anteriores del Ministerio, que sí ha determinado de público conocimiento el Protocolo que se usa para llevar a cabo la intervención de las comunicaciones telefónicas.

Este desequilibrio en la rigurosidad del marco legal también se aprecia si se analiza el *legítimo objetivo de las actividades de vigilancia*. La Ley No. 27.697 señala una lista cerrada de delitos en cuya investigación es posible solicitar la intervención. Dicha lista, que actualmente señala quince delitos, nos permite apreciar que el Estado ha reservado la potestad de afectar el secreto de las comunicaciones exclusivamente en la investigación de los delitos más graves. Por su parte, las leyes de inteligencia sólo reconocen que los mecanismos de intervención podrán ser usados para cualquiera de los objetivos de la actividad de inteligencia (definidos genéricamente como la vigencia de los derechos humanos, proteger a la población de las amenazas contra su seguridad, defender la soberanía nacional, y promover el bienestar general y el desarrollo integral de la Nación).

Ambos sistemas coinciden en exigir un análisis de *necesidad, idoneidad y proporcionalidad* al momento de ordenar las actividades de vigilancia, ya sea a través de la justificación que tiene que enviar el fiscal al juez o en la solicitud que el Director de Inteligencia Nacional envía al juez especial. En el caso del sistema penal, se exige que tanto la Policía como el Fiscal estén obligados a individualizar las medidas solicitadas, las personas afectas, el período durante el cual se llevará a cabo la vigilancia y la presencia de indicios delictivos suficientes.

Del otro lado, las leyes de inteligencia exigen que el pedido de obtención de información identifique a las personas afectadas, señale las medidas que se solicitan así como su duración, y motive las razones del pedido. En términos de proporcionalidad, además, ambos sistemas obligan a las autoridades encargadas de la interceptación la destrucción de todo el material recopilado que no resulte de relevancia para la investigación. Sin embargo, mención aparte merece el mecanismo de retención de datos, que al abarcar la totalidad de los datos relacionados con las comunicaciones de todos los peruanos no ha demostrado ser necesario, idóneo ni proporcionado.

De la misma manera, ambos sistemas cumplen con señalar una *autoridad judicial competente* e independiente para que reciba, evalúe y autorice los pedidos de intervención de las comunicaciones. En el caso del sistema penal, se trata del juez de la investigación preparatoria que es nombrado en forma independiente por el Poder Judicial y es incluso distinto del juez que, de iniciarse un proceso, conocerá el fondo de la denuncia penal. Por su parte, el sistema de inteligencia determina que las solicitudes de obtención de información deben de ser dirigidas a uno de los dos Jueces Superiores Ad hoc del Poder Judicial, designados por la Corte Suprema de Justicia de la República exclusivamente para conocer estas solicitudes.

Lamentablemente, este requisito no se cumple en el caso del acceso a los datos de geolocalización por parte de la Policía Nacional, en donde se obliga a los operadores a entregar esta información a sola solicitud de la policía únicamente si concurren los siguientes requisitos, flagrante delito, si la pena del delito es mayor de cuatro años de cárcel, y, el acceso a esta información constituye un medio necesario para la investigación.

En lo que respecta al *respeto del debido proceso,* se aprecia que si bien existen garantías de juez independiente, motivación y hasta revisión judicial, no se ha contemplado la publicidad de los expedientes ni durante ni después de llevado a cabo los procedimientos de vigilancia. Es comprensible que en algunos casos la completa publicidad del proceso puede comprometer los objetivos de la investigación pero tampoco existen obligaciones de hacer públicos dichos expedientes en el futuro. Incluso, distintas disposiciones establecen la reserva absoluta de cualquier funcionario público o privado involucrado en las actividades de intervención de las comunicaciones. En el caso del acceso a los datos de geolocalización no existe un proceso previo por lo que hay una afectación flagrante a la presunción de inocencia

o el derecho al juez natural de los afectados por la medida.

Otro principio que sí es satisfecho por el sistema penal pero no por el sistema de inteligencia es la *notificación al usuario.* Así, el Código Procesal Penal señala expresamente que luego de ejecutada la medida de intervención y realizadas las investigaciones inmediatas en relación a sus resultados, se deberá de poner en conocimiento del afectado todo lo actuado. El sujeto cuyas comunicaciones fueron intervenidas puede instar el reexamen judicial, dentro del plazo de tres días de notificado. En cambio, el sistema de inteligencia manda la reserva absoluta de todo lo actuado clasificando toda la información como secreta.

El caso del acceso a los datos de geolocalización por parte de la Policía no solo no existe notificación al usuario sino que se proscribe la posibilidad de que las empresas operadoras revelen su participación en estos supuestos al obligarlos a guardar la reserva de la información compartida.

No existen obligaciones específicas de *transparencia* ni de *control público* de las actividades de vigilancia que lleva a cabo el Estado peruano. Salvo las eventuales notificaciones a las personas cuyas comunicaciones fueron intervenidas bajo el sistema de investigación penal, no existen disposiciones legales que obliguen a las entidades que llevan a cabo estas actividades a informar periódicamente del número, tipo y ámbito de las actividades que llevan a cabo. En el caso del sistema de inteligencia, el único espacio de control que existe es la Comisión de Inteligencia del Congreso pero toda la información que le entrega también es clasificada como secreta. Recientemente, la falta de control sobre las actividades del sistema de inteligencia motivó una crisis política que terminó con la desactivación del Sistema y su próxima reorganización.[35] Esta ausencia de transparencia también se ha notado cuando, en sus eventuales apariciones de prensa, la Policía solo comparte parcialmente la información del número de veces que se solicitó la información de geolocalización. Sin embargo, se omite precisar el número de veces que esta información sirvió para capturar un sospechoso o formalizar una denuncia penal.

En términos de la *integridad de las comunicaciones y sistemas*, existe la obligación específica señalada por el Código Procesal Penal que señala que los concesionarios de servicios públicos de telecomunicaciones deben de otorgar acceso, compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Aunque no se conocen casos públicos en donde esta obligación de interconexión haya sido mal utilizada por el Estado, sí significa una restricción a la libertad de los concesionarios de desarrollar su infraestructura de comunicaciones conforme a sus intereses y garantizar la privacidad de los usuarios de sus servicios.

En lo referente a *salvaguardas para la cooperación internacional*, Perú ha suscrito acuerdos de asistencia judicial en materia penal con veinticinco (25) estados del mundo.[36] Entre otros,

Perú mantiene un tratado sobre el cumplimiento de condenas penales con Estados Unidos desde 1980 y un tratado de extradición desde el 2003. Estos acuerdos reconocen como un acto de cooperación judicial internacional la realización de indagaciones o inspecciones, así como la facilitación de información y elementos de prueba dentro de lo que puede estar comprendido el control de las comunicaciones.

Finalmente, nuestro sistema penal sí contempla *salvaguardas contra el acceso ilegítimo* por parte de particulares. El Código Penal establece penas de hasta ocho años de cárcel para quienes intervengan o escuchen comunicaciones telefónicas o similares con agravantes para cuando se difundan a través de medios de comunicación.

IV.
Recomendaciones de Reforma Legislativa

Son varias las reformas posibles y necesarias que pueden introducirse en nuestra legislación local para compatibilizar los mecanismos de vigilancia estatal aprobados por ley con las obligaciones internacionales que ha asumido nuestro país en materia de derechos humanos. En todos los casos, la finalidad de estas reformas no es debilitar los aparatos de investigación penal o de seguridad nacional. Por el contrario, las siguientes propuestas buscan dotar de legitimidad y equilibrio al poder de vigilancia estatal.

La reforma más urgente es revisar el mecanismo en virtud del cual la Policía Nacional puede acceder a los datos de geolocalización de cualquier usuario. En estos casos debería de exigirse siempre el requisito constitucional de la autorización judicial previa. La subsistencia de un sistema como el descrito por el Decreto Legislativo No. 1182 representa un forado en las garantías al derecho a la privacidad de todos los peruanos. De la misma manera, es necesario replantear la necesidad de mantener un sistema de conservación de datos de tráfico por hasta tres (3) años respecto de las comunicaciones de todos los peruanos.

Resulta necesario detallar la legislación aplicable a las actividades de inteligencia para que resulten bien establecidos los límites aplicables a sus labores y actividades. Así, se necesita que ley precise qué se entiende exactamente por actividades de "obtención de inteligencia", que precise plazos en los cuales la información obtenida será destruida o los criterios según los cuales será eventualmente podría ser con otras instituciones o estado extranjeros.
Además, no puede dejar de mencionarse la disociación existente entre la regulación de las prácticas de vigilancia estatal y la forma en la que estas son llevadas a cabo en realidad. Actualmente, no tenemos elementos para determinar informadamente el nivel de cumplimiento de las garantías legales aplicables a la vigilancia de las comunicaciones.

Para enfrentar este tipo de situaciones sería conveniente la implementación de medidas adicionales de transparencia tales como la publicación de información estadística periódica por parte de la Policía y el Poder Judicial sobre el número de solicitudes de intervención de las comunicaciones que procesan al año, así como el ámbito específico de la intervención solicitada: telefónica, electrónica o de seguimiento. Estas medidas no ponen en peligro la efectividad de las medidas ordenadas y permiten a la ciudadanía ejercer un control democrático acerca del ejercicio por parte de la autoridad de tales facultades. Además, tratándose de un cuerpo legislativo reciente como Decreto Legislativo 1182, este tipo de medidas de transparencia aportan valiosos indicadores para evaluar la pertinencia de las reformas recientes y su utilidad en nuestro contexto.

Los escasos espacios de control señalados, especialmente para las actividades de inteligencia, han motivado una auténtica crisis de gobierno. Durante los primeros meses del 2015, se dieron a conocer a través de informes periodísticos una serie de prácticas y ejercicios de vigilancia en la forma de obtención de información pública y privada llevados a cabo por la Dirección Nacional de Inteligencia contra líderes políticos de oposición. Estas revelaciones motivaron un proceso de reestructuración del Sistema de Inteligencia y la remoción de la Presidenta del Consejo de Ministros.[37]

De la misma manera, debe de precisarse mejor las obligaciones que tienen las empresas de telecomunicaciones y de servicios a través de Internet en este marco. Queda claro que están obligadas a facilitar la intervención y registro de las comunicaciones si es que un juez se lo solicita en el marco de una investigación penal. Sin embargo, sus obligaciones para con el sistema de inteligencia resultan demasiado genéricas y pueden ser mal aprovechadas para fines ajenos a las labores de inteligencia. La ley debería de especificar la forma y límites de los pedidos que realice el órgano de inteligencia a las empresas proveedoras de servicios de comunicaciones.

Finalmente, es necesario que se otorgue de mayor autonomía a la Comisión de Inteligencia del Congreso. Dicha Comisión es la instancia independiente con mayor capacidad de control sobre las labores de inteligencia. Hasta el cierre de esta edición, es muy poco lo que se conoce de su trabajo porque todas sus sesiones son reservadas y sus acuerdos también.
Sin debilitar sus labores de control, podría establecerse obligaciones de transparencia a dicha Comisión para que informe sobre el número de veces que cita a miembros del organismo de inteligencia o jueces especializados, el número de procedimientos especiales de obtención de información que revisa. De esa manera, puede salvarse la brecha de información entre las autoridades encargadas de supervisar las labores de inteligencia y la ciudadanía en general.

1 PEN American Center, Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor, Noviembre 12, 2013, disponible en: https://eff.org/r.ozzn

2 James Staten, The Cost of PRISM Will Be Larger Than ITIF Projects, Forrester Research (blog), Agosto 14, 2014, disponible en: https://eff.org/r.37z0

3 Oscar Castilla, Así funciona Constelación, el sistema de escucha telefónica de la Dirandro, El Comercio, Noviembre 30, 2011, disponible en: https://eff.org/r.e3f2

4 El Congreso peruano censura a la primera ministra por espionaje, El País, Marzo 31, 2015, disponible en: https://eff.org/r.vxsy

5 Miguel Morachimo, Nuevo proyecto de ley quiere derogar la #LeyStalker, Septiembre 18, 2015, disponible en: https://eff.org/r.7z02

6 Frank La Rue, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Naciones Unidas, A/HRC/23/40, Abril 17, 2013, disponible en: https://eff.org/r.8fb6

7 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, Harvard Law Review 193 (1890), disponible en: https://eff.org/r.bbgj

8 Corte Interamericana de Derechos Humanos. Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009.

9 Sentencia del Tribunal Constitucional recaída sobre el expediente No. 00655-2010-PHC/TC. 27 de octubre de 2010. Fundamento jurídico 18, disponible en: http://www.tc.gob.pe/jurisprudencia/2010/00655-2010-HC.html

10 Declaración Universal de Derechos Humanos, Artículo 12.—Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

11 Convención Americana sobre Derechos Humanos, Artículo 11.—Protección de la Honra y de la Dignidad: (1) Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; (2) Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. (3) Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

12 Pacto Internacional de Derechos Civiles y Políticos, Articulo 17.—(1) Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación (2) Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

13 Sentencia del Tribunal Constitucional recaída sobre el expediente No. 6712-2005-HC/TC. 17 de octubre de 2005.

14 Decreto Supremo Nº 013-93-TCC, Texto Único Ordenado de la Ley de Telecomunicaciones.

15 Decreto Supremo Nº 020-2007-MTC, Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones.

16 Ley No. 29733, Ley de Protección de Datos Personales, disponible en: https://eff.org/r.beoh

17 Consejo de Derechos Humanos de Naciones Unidas, El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, A/HRC/27/37, Junio 30, 2014.

18 Declaración Universal de Derechos Humanos, Artículo 19.— Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

19 Convención Americana sobre Derechos Humanos, Artículo 13.— Libertad de Pensamiento y de Expresión:
(1) Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
(2) El ejercicio del derecho previsto en el inciso precedente no puede estarsujeto a previa censura sino a responsabilidades ulteriores, las que debenestar expresamente fijadas por la ley y ser necesarias para asegurar:
(a) el respeto a los derechos o a la reputación de los demás, o (b) laprotección de la seguridad nacional, el orden público o la salud o la moral públicas.
(3) No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales oparticulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.
(4) Los espectáculos públicos puedenser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.
(5) Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

20 Pacto Internacional de Derechos Civiles y Políticos, Artículo 19.—(1). Nadie podrá ser molestado a causa de sus opiniones. (2). Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. (3). El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones que deberán, sin embargo, estarexpresamente fijadas por la ley y ser necesaria para: (a) Asegurar el respeto a los derechos o a la reputación de los demás; (b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

21 Sentencia del Tribunal Constitucional recaída sobre el expediente No. 905-2001-AA/TC. 14 de agosto de 2002.

22 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York: Metropolitan Books, 2014), 179.

23 Frank La Rue, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, A/HRC/23/40, Abril 17, 2013.

24 Sentencia del Tribunal Constitucional recaída sobre el expediente No. 00655-2010-PHC/TC. 27 de octubre de 2010. Fundamento jurídico 19, disponible en: http://www.tc.gob.pe/jurisprudencia/2010/00655-2010-HC.html

25 Asamblea General de Naciones Unidas, El derecho a la privacidad en la era digital, Resolución aprobada por la Asamblea General el 18 de diciembre de 2013, A/RES/68/167.

26 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text y EFF, ARTICLE19, Análisis Jurídico Internacional de Apoyo y Antecendentes de los PrincipiosInternacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal

27 A inicios de febrero de 2015, mientras este informe se finalizaba, el Gobierno Peruano anunció su intención de reestructurar totalmente el Sistema de Inteligencia Nacional. Los resultados de esta reestructuración pueden implicar una renovación parcial o total de las normas legales reseñadas.

28 Existe flagrancia cuando un delito se está cometiendo, se acaba de cometer y hasta 24 horas después de cometido (Código Procesal Penal 259)

29 Proyecto de Ley 04809/2015-CR que propone establecer las reglas de coordinación entre la Policía Nacional del Perú, Ministerio Público y Poder Judicial, en casos de flagrancia delictiva, para acceder a la localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, disponible en: http://www.proyectosdeley.pe/p/4twcy6/

30 El presente proyecto de ley no ha sido aprobado al cierre de este informe.

31 Pierina Chicoma Castro, "En 2 meses la PNP geolocalizó 34 celulares de extorsionadores," *El Comercio*, 8 de febrero de 2016, URL: http://elcomercio.pe/lima/seguridad/2-meses-pnp-geolocalizo-34-celulares-extorsionadores-lima-callao-noticia-1877159

32 Decreto Legislativo 1182, Segunda Disposición Complementaria Final.-Conservación de los datos derivados de las telecomunicaciones. Losconcesionarios de servicios públicos de telecomunicaciones y las entidades públicas relacionadas con estos servicios deben conservar los datos derivados de las telecomunicaciones durante los primeros doce (12) meses en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real. Concluido el referido periodo, deberán conservar dichos datos por veinticuatro (24) meses adicionales, en un sistema de almacenamiento electrónico. La entrega de datos almacenados por un periodo no mayor a doce meses, se realiza en línea y en tiempo real después de recibida la autorización judicial. Para el caso de los datos almacenados por un periodo mayor a doce meses, se hará entrega dentro de los siete (7) días siguientes a la autorización judicial, bajo responsabilidad.

33 Ley No. 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones, Artículo 16.- Obligaciones de las entidades supervisadas,— Las entidades supervisadas se encuentran obligadas a: (...) (e) Conservar por un período de al menos 3 (tres) años después de originada la información realizada con la tasación, los registros fuentes del detalle de las llamadas y facturación de los servicios que explota y con el cumplimiento de normas técnicas declaradas de observancia obligatoria en el país por una autoridad competente, o de obligaciones contractuales o legales aplicables a dichos servicios.

34 Resolución de Consejo Directivo No. 138-2012-CD-OSIPTEL, Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, Artículo 65.- Registro de información de llamadas entrantes. A solicitud del abonado, la empresa operadora está obligada a proporcionar el registro de información de las llamadas entrantes al servicio telefónico del abonado (que comprende en general las comunicaciones de voz que son recibidas por los abonados del servicio telefónico fijo y de los servicios públicos móviles), con una anterioridad no mayor a dos (2) meses de realizada la solicitud. La solicitud deberá ser presentada personalmente por el abonado, en cualquiera de las oficinas de la empresa operadora, verbalmente o por escrito. La empresa operadora podrá permitir otros mecanismos adicionales para la presentación de esta solicitud. La emisión de este registro podrá generar el pago de una tarifa. En el documento que se entregue al abonado se detallará el número llamante, la fecha, la hora de inicio y duración de la comunicación. La empresa operadora podrá entregar esta información, de acuerdo a lo indicado por el abonado, en la propia oficina de la empresa, o en el domicilio señalado por el abonado, mediante un documento impreso, por medios electrónicos, o por cualquier soporte informático que tenga la capacidad de almacenar información, en un plazo máximo de quince (15) días útiles posteriores a la presentación de la solicitud. En caso la empresa operadora se negara a brindar este registro, o no cumpliera con entregarlo en el plazo indicado, el abonado podrá iniciar un procedimiento de reclamo de acuerdo a lo establecido en la Directiva de Reclamos.

35 Gobierno cerrará la DINI por 180 días para su reestructuración El Comercio, 9 de febrero de 2015, disponible en: https://eff.org/r.v79d

36 Ver listado Tratados de asistencia judicial en materia penal suscritos por el Perú, Poder Judicial, disponible en: https://eff.org/r.iofv

37 Gobierno anuncia el cierre de la Dirección Nacional de Inteligencia por 180 días, Agenda País, Febrero 5, 2015, disponible en: http://www.agendapais.com/?p+16718