CONTRA EL

DL 1182

¿Por qué derogar el Decreto Legislativo 1182?

CARLOS GUERRERO
MIGUEL MORACHIMO

hiperderecho

Hiperderecho
Asociación civil peruana sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades en entornos digitales. Fundada en el 2012, ha estado involucrada en el debate público de diferentes asuntos de interés público como libertad de expresión, derechos de autor, privacidad y delitos informáticos.

Carlos Guerrero
Bachiller en Derecho por la Universidad Nacional Mayor de San Marcos. Ha participado como becario en programas de la Universidad de Palermo, del Comité Gestor de Internet de Brasil y de la Escuela del Sur de Gobernanza. Actualmente, se desempeña como investigador de Hiperderecho y secretario general del Youth SIG, una organización de Internet Society que busca difundir el respeto por los Derechos Humanos en entornos digitales

Miguel Morachimo
Abogado por la Pontificia Universidad Católica del Perú. Ha seguido cursos de especialización en Derecho y Tecnología en la Universidad de Europa Central (Hungría) y en la Universidad de Ámsterdam (Holanda). Actualmente, se desempeña como Director Ejecutivo de Hiperderecho.

Algunos derechos reservados
Esta obra esta sujeta a la Licencia Reconocimiento 4.0 Internacional de Creative Commons.
Para ver una copia de esta licencia, visite http://creativecommons.org/licenses/by/4.0/

Foto de la portada: Creative Block (bajo una Licencia Reconocimiento 4.0 Internacional de Creative Commons)

Esta publicación es resultado de un proyecto de investigación e incidencia pública financiado por Media Democracy Fund

Esta publicación fue terminada en mayo del 2016

Asociación Civil Hiperderecho
http://www.hiperderecho.org
hola@hiperderecho.org

RESUMEN EJECUTIVO

La lucha contra la delincuencia es una tarea en la que la sociedad está llamada a jugar un rol importante como colaboradora y facilitadora. Sin embargo, este rol no puede significar despojar a los ciudadanos de derechos fundamentales y vulnerar las garantías constitucionales. Las normas aprobadas por el Poder Ejecutivo a través del Decreto Legislativo 1182 han excedido ese equilibrio y pueden hacer más daño del que pretenden evitar.

El Decreto Legislativo 1182 determina incorrectamente que la información sobre la ubicación de un usuario, obtenida mediante la geolocalización de su teléfono móvil, no forma parte del contenido constitucionalmente protegido del secreto y la inviolabilidad de las comunicaciones. No obstante, como se desprende de la Constitución, de sus leyes de desarrollo y de la jurisprudencia existente, dicha información sí se encuentra igualmente protegida que el contenido mismo de la comunicación. Siguiendo este razonamiento, la norma propone que el acceso a dicha información puede ser ejecutado por la policía sin la necesidad de contar con una autorización judicial previa, estableciendo un mecanismo de aprobación judicial posterior para legitimar esta acción. El artículo 10 de la Constitución contradice esto, al establecer que cualquier procedimiento que involucre el acceso a esta información por parte de un tercero debe de ser autorizado y motivado por un juez.

Además de la inconstitucionalidad de sus medidas, el Decreto Legislativo 1182 interfiere también con la implementación del Nuevo Código Procesal Penal en la medida que resta atribuciones al Ministerio Público de forma ilegítima e invalida de facto normas penales que ya disponían cómo debía ser la solicitud y el acceso a los datos de geolocalización. Todas estas medidas buscan ampararse en la interpretación de que la policía puede actuar de esta manera cuando esté frente a un delito flagrante. Por supuesto, esta interpretación está llena de deficiencias y no tiene sustento en la jurisprudencia nacional.

El Decreto Legislativo 1182 también obliga a las empresas de telecomunicaciones a registrar y conservar los datos relacionados con las comunicaciones de sus usuarios, incluyendo registros de llamadas, navegación por Internet y ubicación geográfica. De esta forma, se ordena crear gigantescas bases de datos privadas que estarán a disposición del escrutinio policial durante el plazo de tres (3) años. Esto no es más que la legalización de la vigilancia masiva e indiscriminada, cuya implementación en estas condiciones no resulta necesaria, idónea ni proporcional a los fines que persigue. En otros países existen actualmente normativas similares que ya fueron derogadas, archivadas o enfrentan procesos para que se evalúe su constitucionalidad.

En atención a todo lo expuesto, es necesario derogar parcialmente el referido Decreto Legislativo en los extremos en los que: (i) permite el acceso sin autorización judicial de la Policía a la ubicación de cualquier usuario de dispositivos móviles, y, (ii) ordena a las empresas de telecomunicaciones a conservar los datos derivados de las telecomunicaciones de sus usuarios por un período de tres años.

1. INTRODUCCIÓN

El 27 de julio de 2015 se publicó el Decreto Legislativo 1182, que regula el acceso y posterior uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de telefonía móvil y dispositivos electrónicos afines, en la lucha contra la delincuencia y el crimen organizado. Además, entre otros ajustes legislativos, crea un mandato de retención y conservación de datos derivados de las telecomunicaciones por un plazo de hasta treinta y seis (36) meses.

En Hiperderecho vemos con mucha preocupación las implicancias negativas de la aplicación de una norma de esta naturaleza pues entre sus mecanismos de funcionamiento se contemplan el acceso y uso de los datos arriba referidos sin un mandato judicial previo y la retención de la totalidad de datos derivados de las telecomunicaciones por un largo período de tiempo.

Este documento busca identificar los puntos más controvertidos de este Decreto Legislativo y ofrecer el sustento legal suficiente para su derogación. El informe está divido en dos secciones, dedicadas al mecanismo de acceso a datos de geolocalización y al mandato de retención de datos respectivamente. Cada sección descompone y controvierte en detalle las premisas subyacentes a cada una de estas propuestas a la luz de la legislación nacional y las fuentes internacionales sobre la materia.

2. EL ACCESO SIN ORDEN JUDICIAL A LOS DATOS DE LOCALIZACIÓN Y GEOLOCALIZACIÓN DE CUALQUIER USUARIO DE DISPOSITIVOS MÓVILES ES INCONSTITUCIONAL

2.1. La ubicación geográfica de una comunicación telefónica está protegida por el secreto de las comunicaciones

Los artículos del 1 al 9 del Decreto Legislativo 1182 (en adelante, el "Decreto Legislativo") crean un mecanismo que permite a la Policía Nacional del Perú acceder de forma inmediata y dar seguimiento en tiempo real al dato de localización o geolocalización de teléfonos móviles o dispositivos electrónicos conectados a una red pública de telecomunicación. Para esto, la norma señala que no necesitan contar con una orden judicial previa ni hacer el pedido a través del Ministerio Público.

Por **datos de localización o geolocalización** se entiende a todos aquellos que se generan al momento en que un teléfono móvil o un dispositivo electrónico se conecta a una red pública de telecomunicaciones y revelan el detalle de su ubicación geográfica. Estos datos son accesibles mediante una técnica llamada localización por triangulación, que es inherente al funcionamiento de cualquier red de comunicaciones celular.[1] En otras palabras, al obtener la ubicación geográfica de un dispositivo móvil puede conocerse el paradero exacto de la persona que use dicho aparato.

Aunque esta información puede parecer trivial, en muchos casos la información de geolocalización de una llamada telefónica o la obtenida del desplazamiento de un teléfono

móvil puede revelar mucho sobre la intimidad de una persona. Piénsese, por ejemplo, en lo que puede inferirse cuando una llamada se realiza desde hospitales, hoteles o centros de recreación nocturna. Cuando esta información es monitoreada en tiempo real durante uno o más días, es fácil apreciar patrones de comportamiento como dónde pasa la noche una persona, a qué sitios suele acudir durante el día y a quiénes visita. En suma, resulta innegable que existe información privada en el dato de localización de una llamada telefónica que es tan merecedora de protección como el contenido mismo de la llamada.

Correctamente, nuestra Constitución señala en su artículo 2 que toda intervención de las comunicaciones o de sus instrumentos está sujeta a una orden judicial previa.[2] Sin embargo, el artículo 6 del Decreto Legislativo 1182 hace énfasis en que este nuevo mecanismo no pretende realizar ningún tipo de intervención, pues "solo" busca acceder al detalle de la ubicación geográfica del dispositivo móvil. Esto equivale a decir que **el Decreto Legislativo no reconoce que los datos de geolocalización forman parte del contenido protegido por el secreto e inviolabilidad de las comunicaciones** que se cita en el texto constitucional. Bajo su lógica, el acceso a los mismos no estaría sujeto a la formalidad establecida para ese tipo de intervenciones. Resulta más que evidente que esta interpretación restrictiva busca evitar la inconstitucionalidad del Decreto Legislativo negando un hecho evidente: los datos de geolocalización se derivan de un acto directamente relacionado con el proceso de la comunicación (en este caso, el acto de conectar el dispositivo a la red pública de telecomunicación), siendo entonces de la misma naturaleza que otros datos como la hora de una llamada o su duración, cuya protección bajo el secreto de la comunicaciones es innegable.

El Tribunal Constitucional ha expresado su oposición a esta interpretación al reconocer que el contenido constitucionalmente protegido del derecho al secreto y la inviolabilidad de las comunicaciones no solo comprende el contenido mismo de la comunicación sino también todas las operaciones que la hacen posible. Así, se ha señalado como comprendidas la identidad de los participantes de la comunicación,[3] o "datos externos del mensaje, como los nombres de los participantes, la entidad a la que puedan pertenecer, la dirección de origen o de destino, los códigos o números que identifican a los participantes, entre otros". [4]

Inclusive, el mismo Tribunal ha llegado a hacer suya la definición de la Corte Interamericana de Derechos Humanos que señala que no solo se protege el contenido de las comunicaciones sino también cualquier otro elemento u operación técnica relacionada:

> La Corte Interamericana de Derechos Humanos en la sentencia del Caso Escher y otros vs. Brasil, del 6 de julio de 2009, ha precisado que el derecho a la vida privada previsto en el artículo 11° de la Convención Americana sobre Derechos Humanos protege "las conversaciones realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio o actividad profesional que desarrolla.
> De ese modo, 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.[5]

Asimismo, en el ordenamiento interno encontramos leyes de desarrollo como la Ley General de Telecomunicaciones, que repite en su artículo 4 que toda persona tiene derecho a la inviolabilidad y al secreto de las telecomunicaciones.[6] En el mismo sentido, su Reglamento, aprobado mediante Decreto Supremo 020-2007-MTC, señala expresamente que se atenta contra el secreto e inviolabilidad de las telecomunicaciones cuando se conoce de la existencia o se accede al contenido de cualquier comunicación.[7] Es decir, la sola noticia de que una comunicación se estableció entre dos partes ya es reconocida como protegida por el secreto de las comunicaciones.

De igual forma, desde el año 2009 contamos con una norma especial aprobada por el Ministerio de Transportes y Comunicaciones que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones. Esta señala expresamente como parte del ámbito de protección del derecho al secreto e inviolabilidad de las telecomunicaciones "el origen, destino, realización, curso o duración de una comunicación".[8]

En resumen, existe un amplio desarrollo jurisprudencial y normativo que permite una interpretación amplia de los elementos protegidos por el secreto de las comunicaciones, pudiendo ubicar los datos de geolocalización dentro de esta categoría. En ese sentido, el extremo del Decreto Legislativo que no reconoce dicha protección y trata como externo a dicho elemento constituye una interpretación en contra del texto constitucional.

2.2. El acceso a la localización o geolocalización solo puede ser autorizado y motivado por un Juez

Como quedó claro en el punto anterior, los datos de ubicación geográfica sí están protegidos por el secreto y la inviolabilidad de las comunicaciones. No obstante, como ocurre con cualquier derecho, esta protección no es absoluta y por lo tanto puede ser limitada bajo ciertos supuestos que deben encontrarse tipificados en la ley y responder a la satisfacción de otros derechos de igual o superior jerarquía.

En el presente caso, dicho límite viene impuesto por un lado por la Constitución, que establece como requisito previo la existencia de un mandato judicial que ordene el acceso. Por otro, en normas que contienen dispositivos restrictivos de derechos y que establecen pautas procedimentales, como es el caso del Código Procesal Penal que en su artículo 230 establece los supuestos en los que un fiscal puede solicitar al juez la intervención de las comunicaciones.[9]

El Tribunal Constitucional ha sido claro a la hora de señalar la importancia del principio de judicialidad, que no es sino la garantía de la aplicación imparcial y correcta de la ley penal

por parte del juez. Así pues, las actuaciones de la Policía en materia de intervención de las comunicaciones que no se encuentren amparadas en una orden judicial previa suponen no solo una afectación directa a los derechos de los intervenidos sino que son fuente de obtención de pruebas ilícitas que no pueden usarse dentro de un proceso.

De modo ilustrativo, podemos mencionar uno de los fundamentos de la sentencia recaída sobre el expediente No. 1058-2004-AA/TC[10] en donde el Tribunal reafirma estos conceptos al señalar que los elementos probatorios obtenidos mediante la vulneración ilegítima de un derecho no pueden ser usados en ningún tipo de proceso pues su presencia desnaturaliza los derechos de las personas y vuelve nulos todos los actos que su existencia pudiera haber generado.

Por todo ello, no cabe duda de que el papel del juez es clave en tanto que, en el caso de la afectación al secreto e inviolabilidad de las comunicaciones, la Constitución le reconoce a él la función exclusiva de decidir en qué casos y bajo qué condiciones autoriza el acceso al contenido o a los instrumentos de la comunicación. No obstante, el Decreto Legislativo 1182 es consecuente en su primera equivocación y niega también la necesidad de que el acceso pase antes por un control judicial que le otorgue legitimidad. Al desconocer esto, la inconstitucionalidad aparente de todo este extremo de la norma se vuelve total. Por supuesto, este obstáculo se intenta salvar mediante la introducción de la flagrancia delictiva, pero ese punto se analizará más adelante.

Un elemento que llama la atención es que el Decreto Legislativo 1182 sí considera una etapa de "convalidación judicial," luego de que se ha producido el acceso a los datos de geolocalización. Es decir, aunque considera que esa información no se encuentra protegida por la garantía de la inviolabilidad de las comunicaciones, de todas maneras establece que un juez revise su legalidad de manera posterior. A todas luces, el Decreto reconoce implícitamente lo sensible de esta información y es por ello que busca una convalidación judicial posterior a la medida. Precisamente porque esta información es sensible es que la Constitución establece la garantía del acceso previa orden judicial, no posterior.

2.3. La "fórmula" de la flagrancia presenta serios problemas de aplicación de cara al acceso a los datos de ubicación y a la detención policial

Habiendo admitido que los datos de geolocalización se encuentran protegidos por el secreto de las comunicaciones y que solo un juez puede disponer el acceso a los mismos, los proponentes del Decreto Legislativo pretenden superar el 'obstáculo' de la inconstitucionalidad de sus normas amparándose en la excepcionalidad de la flagrancia delictiva. Con este propósito, el artículo 3 del Decreto Legislativo establece los supuestos bajo los cuales la Policía Nacional puede acceder a los datos de ubicación geográfica de cualquier dispositivo móvil sin mandato judicial previo, siendo estos los mismos que figuran en el artículo 230 del Código Procesal Penal (pena mayor a 4 años y necesidad de la medida), pero añadiendo la flagrancia como nueva condición.

Para poder entender el problema implícito de la inclusión de esta figura conviene recordar que nuestro ordenamiento no tiene una definición explícita de flagrancia. Sin embargo,

podemos interpretar su contenido de las situaciones mencionadas de forma taxativa en el artículo 259 del Código Procesal Penal.[11]

Ante situaciones de flagrancia delictiva, la Policía Nacional puede vulnerar ciertos derechos sin la necesidad de un mandato judicial (como ocurre en el caso de la libertad de tránsito o la inviolabilidad del domicilio). El Decreto Legislativo busca en esta interpretación una vía para evadir la inconstitucionalidad a la que nos hemos referido anteriormente. Sin embargo, como hemos señalado, este razonamiento presenta dos problemas:

- Una lectura integral de la Constitución permite observar que tanto la libertad personal, la inviolabilidad del domicilio como el secreto de las comunicaciones, en tanto derechos fundamentales, son reconocidos expresamente por el texto constitucional. Sin embargo, solo en los dos primeros casos se reconoce a la flagrancia como una causal legítima de vulneración de dichos derechos, por lo que no se hace necesario contar con una orden judicial. En cambio, no hay ninguna parte del texto constitucional que autorice la vulneración del derecho a la inviolabilidad de las comunicaciones como lo propone el Decreto Legislativo 1182. En otras palabras, estamos frente a una norma de rango legal que intenta incluir una excepción a un derecho fundamental que estaría al nivel de las otras dos excepciones constitucionales.[12]
- El segundo problema es que, en la práctica, el mecanismo establecido en el Decreto Legislativo convierte a cualquier declaración de un tercero en elemento suficiente para crear convicción de que tal flagrancia existe, facultando así a la Policía Nacional a acceder a los datos de geolocalización y, eventualmente, proceder a la captura del o los presuntos delincuentes. En esa misma línea de ideas, es lógico pensar que en la mayoría de casos, sino en todos, existirá por parte de la Policía un interés porque el acceso sea "legítimo" a toda costa, es decir, que se justifique con la captura de alguien que efectivamente ha cometido un delito, siendo que en caso contrario los agentes que autorizaron la intervención pueden ser pasibles de sanción. Al respecto de este punto, hay que señalar también que El Tribunal Constitucional ha establecido que para poder hablar de la existencia de un supuesto de flagrancia delictiva es necesario que se cumplan al menos dos requisitos: el de inmediatez temporal o personal[13], que ciertamente no se cumplirían en la mayoría de casos en los cuales no existe algún tipo de investigación previa, pues al basarse la convicción policial en la declaración de un tercero y estar sujeta a las limitaciones de la geolocalización, podrían incluso resultar infructuosas o contraproducentes.

En buena cuenta, el Decreto Legislativo interpreta que si bien la libertad de tránsito y la inviolabilidad del domicilio son derechos fuertemente protegidos por la Constitución, su vulneración en casos de flagrancia delictiva es legítima. Por lo tanto, debe extrapolarse que debe ocurrir lo mismo en el caso del secreto e inviolabilidad de las comunicaciones, lo que evita que sus mecanismos devengan en inconstitucionales. Por supuesto, este razonamiento es incorrecto en la medida que en todos los demás casos, la figura de la flagrancia se establece expresamente, no ocurriendo lo mismo en lo referente a las comunicaciones. Además, una interpretación teleológica apoya la tesis de que la mediación judicial en estos

supuestos fue siempre deseable, lo que llevó a no incluir la flagrancia dentro de los supuestos de afectación de este derecho.

Asimismo, cuestiones relativas a la aplicación presentan problemas críticos en la medida que la Policía Nacional no tiene manera de crearse convicción antes de acceder a los datos de geolocalización, derivando incluso en la invalidez de las detenciones preventivas o sustentadas en meras sospechas.[14] De la misma forma en aquellos casos en donde entra en juego la "ventana de tiempo" de la flagrancia, que otorga solo veinticuatro horas de margen para actuar, o en donde la captura se torne en irrealizable pues el mecanismo propuesto por el Decreto Legislativo no es lo suficientemente exacto para vencer obstáculos técnicos como los que representan grandes concentraciones de personas o edificios de varios pisos. Por ello es que esta "solución" trae más problemas de los que resuelve y, en el mejor caso, vuelve a la norma muy inefectiva.

2.4. El procedimiento de convalidación judicial posterior no satisface las garantías constitucionales

Otro de los puntos de debate del Decreto Legislativo es la cuestión relativa a la revisión judicial posterior de las actuaciones policiales en torno al acceso de los datos de geolocalización que propone. Estas intervenciones no solo son, a nuestro parecer, ilegítimas, sino que el hecho mismo de apartar a los jueces de su rol de control previo tiene como consecuencia la inobservancia de ciertas garantías constitucionales.

Una de ellas es la vulneración al derecho al debido proceso que, según el desarrollo constitucional, supone la afectación del cumplimiento de las garantías, requisitos y normas de orden público que deben observarse en todas las instancias procesales. Lo que ciertamente ocurre bajo el mecanismo propuesto por el Decreto Legislativo en dos instantes: (i) en el momento del acceso a los datos, y, (ii) cuando surge la pretensión de incluir medios de pruebas derivados de esta intervención dentro de un proceso. En el caso de estos últimos, se afectaría también la garantía de publicidad de los expedientes dado que el Decreto Legislativo no ha contemplado la posibilidad del acceso a la información relativa a la intervención ni durante ni finalizado el proceso.

Respecto del derecho al debido proceso, César Landa Arroyo afirma que "el debido proceso encierra en sí un conjunto de garantías constitucionales que se pueden perfilar a través de identificar las cuatro etapas esenciales de un proceso: acusación, defensa, prueba y sentencia, que se traducen en otros tantos derechos."[15] En ese sentido, el modelo del Decreto Legislativo no estaría garantizado tampoco un acceso eficaz a los medios de defensa de las personas afectadas por estas medidas.

Otra de las garantías afectadas viene a ser la presunción de inocencia, cuyo contenido no es sino presumir la inocencia de una persona hasta que su culpabilidad quede demostrada en un juicio. Esta misma es violentada en el momento en que la Policía Nacional decide, bajo sus propios criterios, acceder a los datos de ubicación geográfica pues esto implicará en muchos casos una valoración jurídica de culpabilidad (siendo el acceso a la ubicación el modo en que esta podrá o no ser justificada), que no les corresponde.

En resumen, el mecanismo del Decreto Legislativo que ordena que la convalidación judicial se realice de forma posterior al acceso a los datos de geolocalización por parte de la Policía Nacional no solo pervierte el rol de garantes que tienen los jueces sino que afecta garantías constitucionales como el debido proceso y la presunción de inocencia. El primero es afectado en tanto que el proceso supone el respeto de los procedimientos y funciones de sus actores, algo que el Decreto Legislativo rompe al intercambiar roles a su discreción. El segundo es afectado también en la medida que el acto mismo del acceso constituye una suerte de "juzgamiento previo" por parte de la Policía, pues ya hemos señalado que una mera declaración o suposición de la flagrancia no es un elemento suficiente para crearse convicción y por lo tanto proceder de forma legítima.

2.5. Ya existe un mecanismo legítimo para acceder a la información de localización y geolocalización de cualquier teléfono móvil

Es innegable que en ciertos casos resulta necesario acceder a la ubicación de un teléfono móvil en el contexto de la investigación criminal y la lucha contra la delincuencia. Es por esto que desde el año 2014 existe en el artículo 230 del Código Procesal Penal un proceso especial para acceder a esta información.[16] Este artículo señala que esta información puede ser solicitada por un Fiscal al Juez de la Investigación Preparatoria siempre que concurran dos supuestos: (i) suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años, y, (ii) que se considere absolutamente necesario para proseguir las investigaciones. El citado artículo también señala que los concesionarios de servicios públicos de telecomunicaciones deben 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.

Por el contrario, el Decreto Legislativo 1182 desconoce el procedimiento reseñado y crea un mecanismo alternativo que debilita la finalidad del acceso a los datos de geolocalización al circunscribirlo exclusivamente a la Policía. Así, desde la entrada en vigencia del Decreto Legislativo 1182, la Policía Nacional ha pasado a tener mayor poder que el propio Ministerio Público, que todavía necesita de una orden judicial para acceder a la información de geolocalización según el Código Procesal Penal.

El Decreto Legislativo 1182 no es realmente una solución al problema o, en todo caso, es una solución parcial pues no mejora los mecanismos ya existentes sino que intentan superponerse a ellos. Así, en lugar de sumar esfuerzos para lograr una mayor articulación entre las diferentes dependencias que intervienen en la lucha y procesamiento de la delincuencia (Poder Judicial, Ministerio Público, Policía Nacional), la propuesta solo busca empoderar en grado máximo a la Policía, asignándoles a los demás actores simples tareas de validación.

2.6. El procedimiento de geolocalización no tiene mecanismos de transparencia

Tal como está descrito en el Decreto Legislativo 1182, el procedimiento de geolocalización carece de mecanismos de transparencia y de rendición de cuentas que validen su efectividad. Sin una efectiva rendición de cuentas sobre el número de veces que se lleva a cabo este procedimiento y su tasa de éxito, resulta imposible que la sociedad evalúe su verdadera utilidad para la persecución de delitos.

El Decreto Legislativo contempla dos formas de revisión para el procedimiento de acceso a datos de geolocalización: la convalidación judicial y la auditoría operativa. Aunque estos mecanismos de revisión pueden servir para evaluar el cumplimiento de la norma, no son útiles para analizar su efectividad a mediano plazo. La primera se lleva a cabo hasta 72 horas después de solicitado el acceso a la empresa operadora y se realiza bajo trámite reservado. De la misma manera, la auditoría operativa se lleva a cabo por las inspectorías generales del Ministerio del Interior y de la Policía Nacional, que no están obligadas a poner a disposición del público los resultados de sus informes.

En su declaración conjunta sobre programas de vigilancia, los relatores especiales para la Libertad de Expresión de Naciones Unidas y de la Organización de los Estados Americanos han señalado expresamente que las leyes deben de asegurar que el público en general pueda acceder a la información sobre programas de vigilancia de las comunicaciones, incluyendo la correspondiente al uso de estas herramientas y estadísticas generales sobre su alcance.[17] Así mismo, el citado Reporte establece que los estados deben de mantener mecanismos de supervisión independientes y capaces de asegurar la transparencia y rendición de cuentas de los programas de vigilancia.

2.7. La información sobre geolocalización de un teléfono no siempre es útil para la persecución de delitos

Incluso asumiendo que todos los problemas legales de esta propuesta se solucionaran, todavía existen condiciones técnicas que discuten la idoneidad de la medida. La lógica subyacente al mecanismo establecido por el Decreto Legislativo es que los delincuentes van a usar un solo teléfono y lo van a tener todo el tiempo consigo durante y luego de la comisión de un delito. De esta manera, el Decreto Legislativo asume que si puede ubicarse el origen de una llamada podrá darse con el paradero de un delincuente. Esta es una afirmación que no siempre es cierta.

Por ejemplo, si el delincuente usa un teléfono fijo, un teléfono público o un teléfono originado desde un sistema de Voz sobre IP (ej. Skype), la información sobre la ubicación de dicho terminal va a ser poco útil o, si la llamada se originó desde Internet, resultará imposible de obtener.

En otros casos, la información sobre geolocalización de un teléfono móvil puede resultar poco útil para ubicar a un criminal si es que la llamada se hace desde un lugar con una gran concentración de personas, como una plaza, un mercado o un espacio con múltiples pisos como un edificio. Igualmente, el delincuente podría optar por abandonar el aparato terminal luego de realizar la llamada con lo que su geolocalización no serviría de mucho. En

general, existen múltiples "precauciones" que puede tomar un delincuente si es que no desea ser geolocalizado y que el Decreto Legislativo parece ignorar.

3. LA RETENCIÓN DE DATOS DERIVADOS DE LAS TELECOMUNICACIONES DE TODOS LOS PERUANOS AFECTA LA PRIVACIDAD Y ES DESPROPORCIONADA E INNECESARIA

En su sección de disposiciones complementarias finales, el Decreto Legislativo establece la obligación de los operadores de telecomunicaciones de conservar los datos derivados de todas las telecomunicaciones de sus usuarios durante un período de tres (3) años. Al respecto, precisa que los operadores deberán establecer un sistema que permita a la Policía Nacional acceder a estos datos en tiempo real durante los primeros doce (12) meses. Para el caso de datos almacenados por un período mayor, el acceso tendrá un período de respuesta máximo de siete (7) días. En ambos casos, el acceso se tramitará solo mediante autorización judicial.

La norma no define lo que entiende por "datos derivados de las telecomunicaciones." Sin embargo, por la amplitud del término debe de asumirse que se trata de toda la información que es procesada por una empresa de telecomunicaciones durante el acto mismo de la comunicación. Es decir, este criterio abarca no solo la información sobre la geolocalización de una comunicación sino también su duración, identificación de los titulares de la comunicación, identificadores únicos de los terminales utilizados, tráfico de datos, entre otros. De la misma manera, debe entenderse que este mandato abarca no solo las llamadas telefónicas sino todos los servicios clasificados en nuestro país como servicios públicos de telecomunicaciones (telefonía fija, telefonía móvil, telefonía pública, acceso a Internet, distribución de radiodifusión por cable, entre otros). La citada disposición no discrimina entre los servicios públicos de telecomunicaciones que estarán sujetos a esta obligación por lo que debe de entenderse que son todos. De la misma manera, tampoco diferencia entre usuarios de servicios públicos sujetos a este mecanismo por lo que debe entenderse que aplica a todos los usuarios sin importar su nacionalidad, profesión, filiación política o edad.

En pocas palabras, el Decreto Legislativo 1182 obliga a las empresas prestadoras de servicios públicos de telecomunicaciones a conservar todos los datos derivados de todos los servicios de comunicaciones como registros de llamadas, ubicación geográfica, horarios, e incluso volumen y tipo de tráfico cursado a través de Internet. Esto significa que para cada usuario de servicios públicos de comunicaciones existirá en todo momento un registro personal de hasta tres años antes conteniendo una lista detallada de sus hábitos de comunicación, de navegación en Internet, desplazamiento y de círculos sociales. Internacionalmente, las obligaciones de este tipo son denominadas **mandatos de retención o conservación obligatoria de datos**.

3.2. La retención obligatoria de datos derivados de las telecomunicaciones afecta la privacidad

La información que el Decreto Legislativo 1182 obliga a las empresas de telecomunicaciones a almacenar es información privada. Los datos "derivados de las telecomunicaciones" o metadatos constituyen un reporte detallado de hábitos,

desplazamientos e interacciones sociales que bien pueden ser analizados para determinar preferencias religiosas, condiciones médicas, relaciones afectivas, manifestaciones políticas, entre otras. Como se demuestra en este acápite, su recopilación extensiva y detallada constituye una vulneración al derecho a la privacidad.

El derecho a la privacidad está ampliamente reconocido como aquel en virtud del cual las personas no deben ser sujetas a injerencias arbitrarias a su vida privada por parte de autoridad o terceros. En esos términos lo entiende el artículo 12 de la Declaración Universal de los Derechos Humanos,[18] el artículo 11 de la Convención Americana de Derechos Humanos[19] y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.[20] Nuestra Constitución recoge también parte de estas acepciones en su texto, referidas sobre todo al derecho a la intimidad personal y familiar.

La práctica de retención de datos incide directamente sobre este derecho. Tal como lo han señalado las relatorías para la libertad de expresión de Naciones Unidas y la OEA en su "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión," la recolección de los metadatos de las comunicaciones digitales equivale a una limitación a la intimidad y la vida privada en tanto que estos son altamente reveladores. [21] De forma más concreta, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos indicó que los metadatos puedan dar una mejor idea del comportamiento, relaciones sociales, referencias e identidad de una persona, incluso más que el contenido mismo de la comunicación.[22] En el mismo sentido se ha pronunciado también el Relator Especial para la Libertad de Expresión de Naciones Unidas en su reporte del 2013 al señalar:

> Las leyes nacionales de conservación de datos son invasivas y costosas, y atentan contra los derechos a la intimidad y la libre expresión. Al obligar a los proveedores de servicios de comunicaciones a generar grandes bases de datos acerca de quién se comunica con quién telefónicamente o por Internet, la duración del intercambio y la ubicación de los usuarios, y a guardar esta información (a veces durante varios años), las leyes de conservación obligatoria de datos aumentan considerablemente el alcance de la vigilancia del Estado, y de este modo el alcance de las violaciones de los derechos humanos. Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental.[23]

Una medida que crea la obligación de retener y conservar grandes bases de datos de los usuarios de servicios de telecomunicaciones vulnera el derecho a la privacidad en el sentido que estas operaciones son realizadas sin expresión de causa, no se aprecian mecanismos de salvaguarda de la información y existe un inminente peligro de sustracción y uso indebido. Lo último conllevaría a nuevas afectaciones ilegítimas a otros derechos de personas sobre las cuales no existe ninguna investigación o proceso en curso.

En este punto, es pertinente precisar que la afectación a la privacidad se produce por la mera recolección de la información sin que importe si esta fue realmente leída o utilizada por terceros. Así lo ha precisado el Informe de la Oficina del Alto Comisionado de las

Naciones Unidas para los Derechos Humanos cuando precisa que "la recopilación y conservación de datos de las comunicaciones equivale a una injerencia en la vida privada, independientemente de si posteriormente se consultan o utilizan esos datos."[24] En el mismo sentido se ha expresado el Relator Especial de Naciones Unidas sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo al señalar que "la recopilación y conservación de los datos de tráfico de las comunicaciones constituye una injerencia en el derecho a la privacidad, independientemente de si posteriormente una autoridad pública accede a ellos y los analiza o no."[25]

Además de su evidente impacto en la privacidad, las prácticas de retención de datos también pueden afectar el libre ejercicio de otro derechos como el de la libertad de expresión o de reunión. Al someter a todos los usuarios de servicios de telecomunicaciones a un régimen de monitoreo constante, estos pueden terminar modificando su conducta al reprimirse de circular por ciertas áreas o evitar acceder a cierto tipo de información a través de Internet. En el largo plazo, esta auto censura deliberada o involuntaria puede tener efectos gravísimos para la democracia, la diversidad de opiniones y el estado de Derecho en nuestro país.

3.3. La retención obligatoria de datos derivados de las telecomunicaciones es desproporcionada

Antes de la promulgación del Decreto Legislativo, los operadores de servicios de telecomunicaciones tenían dos obligaciones relativas a la conservación de los datos generados por sus usuarios:

- La primera de ellas es la que emana de la Ley No 27336 y que ordena la conservación de por los menos tres (3) años de la información referida a la tasación, los registros fuente del detalle de llamadas y la facturación de los servicios con fines de supervisión por parte del Organismo Supervisor de las Telecomunicaciones (OSIPTEL).[26]
- La segunda, algo más implícita, emana de las "Condiciones de Uso de los Servicios Públicos de Telecomunicaciones", resolución emitida por el Consejo Directivo del OSIPTEL y de cumplimiento obligatorio de los operadores, que señala que los abonados del servicio tienen derecho a solicitar a estos su detalle de llamadas entrantes con hasta dos (2) meses de antigüedad al momento de la solicitud.[27]

En ambos casos se advierte una obligación de conservar información de llamadas y facturación, el primero con motivos de supervisión por parte del OSIPTEL y el segundo en función al correcto cumplimiento del servicio y el hacer más fácil al usuario obtener herramientas de reclamación para el usuario. En ninguno de los dos casos se deja entender que la finalidad o el uso de estos datos pueden extenderse hasta abarcar fines investigación criminal que, de ser el caso, deberían estar plasmados en leyes penales y no en disposiciones de carácter administrativo. De la misma manera, las dos obligaciones existentes se circunscriben exclusivamente a los servicios públicos de telefonía fija o móvil.

En cambio, el Decreto Legislativo 1182 crea el mecanismo de retención de datos con el fin de combatir la delincuencia y garantizar la seguridad y el orden público, dos fines perfectamente legítimos. Sin embargo, esta finalidad se ve desnaturalizada porque el mecanismo no cumple con requisitos mínimos que aseguren que las vulneraciones serán selectivas y limitadas. Muy por el contrario, las bases de datos que propone crear esta norma abarcan a todo el universo de usuarios sin distinción, incluyen todos los datos generados (ya no solo el registro de llamadas) y extienden la afectación por un período de 3 años. Esto configura una respuesta desproporcionada por parte del Estado que merece al menos ser revisada y perfeccionada para incluir todas estas observaciones.

En esa misma línea, la Declaración conjunta sobre la libertad de expresión y las respuestas a las situaciones de conflicto, firmada por los Relatores Especiales de la ONU, OSCE, OEA, y de la Comisión Africana señala de forma contundente que:

> (…) la obligación de retener o las prácticas de retención de datos personales de forma indiscriminada con el fin de mantener el orden público o por motivos seguridad no son legítimos. En cambio, los datos personales deberían ser retenidos con fines de orden público o para temas de seguridad solo de forma limitada y selectiva y en una forma que represente un equilibrio adecuado entre los agentes del orden público y la seguridad y los derechos a la libertad de expresión y a la privacidad.[28]

3.4. El Poder Ejecutivo no ha acreditado que la conservación de los datos sea necesaria

En su Exposición de Motivos, el Decreto Legislativo pretende explicar por qué un mecanismo de retención y conservación de datos derivados de las telecomunicaciones es necesario para combatir a la delincuencia y el crimen organizado.[29] Para ello, se basa en que existen reportes de la Policía Nacional que constatan que el uso de equipos de comunicación de telefonía móvil para cometer delitos se ha incrementado en el año 2015. Afirma también que tanto el *modus operandi* como las organizaciones criminales están plenamente identificados, pero no existe un marco legal de actuación para que la policía pueda efectuar acciones disuasivas y preventivas. Para respaldar este argumento, el texto viene acompañado por dos cuadros estadísticos de incidencia delictiva, el primero del año 2014 y el segundo de los meses de enero hasta julio del año 2015.

Estas afirmaciones omiten información importante. En principio, es falso que no exista un marco de actuación policial pues, como lo hemos mencionado a lo largo de este informe, empezando por la Constitución y en el desarrollo de las normas penales, queda claro cuáles son los procedimientos en caso se necesite el acceso a los datos protegidos por el secreto e inviolabilidad de las comunicaciones.

Además, los cuadros estadísticos son solo registros de incidencia criminal, y en ninguna parte se puede visualizar individualizaciones de los delitos que estarían cometiéndose con el uso de equipos de telefonía móvil. Tampoco se presentan cifras o estudios relativos al aumento del uso de estos equipos para cometer delitos, siendo algo vital para aceptar el

argumento como cierto pues el uso de teléfonos móviles está extendido en la población y afirmar que "los delincuentes también los usan" no equivale a decir que estos están relacionados necesariamente con la comisión de delitos. Finalmente, no se añaden precisiones acerca de cuántos pedidos de acceso a los datos de geolocalización ha hecho la Policía hasta la fecha para medir objetivamente la necesidad de implementar los mecanismos de conservación que propone el Decreto Legislativo.

Entonces, ¿cuál es el verdadero contexto en el que se plantea la necesidad de estas medidas? Haciendo uso de fuentes oficiales, pasamos a señalar algunos datos importantes para evaluar en qué medida estos mecanismos satisfacen realmente una necesidad de la Policía Nacional para combatir contra la delincuencia.

En lo que respecta al número de delitos cometidos, incidencia criminal y número de denuncias a nivel nacional, el Anuario Estadístico de la Policía Nacional del Perú del año 2014 presenta cuadros estadísticos que revelan esta realidad[30] siendo algunas de sus conclusiones que, efectivamente, el número de denuncias con respecto al año 2013 ha aumentado en 3.79%, siendo que los delitos más denunciados son aquellos cometidos contra el patrimonio (hurto, robo, apropiación ilícita, estafas, otros).[31] De ello podemos colegir que el crecimiento del número de delitos ha sido constante al menos en los dos últimos años y que, por diversos motivos, los planes de acción policial no han sido lo suficientemente eficaces para detener este crecimiento. Así mismo, es claro por las estadísticas que la mayoría de estos delitos se concentra en la ciudad de Lima y algunas ciudades del norte como Trujillo, y los más recurrentes son los delitos contra el patrimonio que además, según el mismo informe, son los de mayor visibilidad social.

No obstante, hay que señalar al menos como dato referencial que, según los resultados definitivos del III Censo Nacional de Comisarías 2014[32], existen otras necesidades que podrían estar restando capacidad operativa a la Policía en su lucha contra el crimen. Algunos datos resaltantes son que casi el 40% de comisarías censadas no dispone de servicios básicos adecuados como agua potable, desagüe y energía eléctrica de forma permanente, que más de la mitad no poseen teléfonos fijos ni tampoco acceso a la base de datos de la RENIEC y que solo el 38,5% cuentan con conexión propia y adecuada a Internet.

Teniendo en cuenta esta muestra habría que preguntarse si es que el supuesto negado de "la falta de marcos legales adecuados" es el principal problema que encuentra la Policía Nacional para combatir la delincuencia. Más aún, cuando las cifras nos indican que más de la mitad de los delitos cometidos en el país se concentra en Lima y son en abrumadora mayoría delitos contra el patrimonio. El aumento de la sensación de inseguridad encuentra su correlato en el hecho de que la incidencia criminal sí ha aumentado, pero de ninguna forma esto respalda la idea de que conservar los datos de las telecomunicaciones garantiza alguna disminución significativa del crimen (teniendo en cuenta que la ley tiene alcance nacional). Por lo tanto, semejante intromisión con respecto al derecho a la privacidad no está justificada, sin dejar de mencionar los riesgos de fuga y de mal uso a los que estarían expuestos.

En pocas palabras, en la Exposición de Motivos, se ensayan tres argumentos para justificar la necesidad de la conservación de datos: (a) que las tecnologías de comunicación estarían siendo empleadas por delincuentes y organizaciones criminales, (b) que en los últimos meses la comisión de delitos cometidos bajo esta modalidad ha aumentado drásticamente, y, (c) el marco legal vigente no favorece a la actuación policial. Como ya hemos reseñado, sobre los dos primeros puntos solo existen cifras vagas y genéricas que no prueban fehacientemente la relación entre el uso de dispositivos móviles y el aumento del crimen. Incluso existen otros datos que hablan de diferentes carencias de la Policía Nacional que también entorpecen su labor. Con respecto al marco legal, afirmamos que este ya existe y, en todo caso, no se han presentado información oficial que permita suponer que la Policía Nacional ha visto frustrada sus operaciones por la falta de aprobación de solicitudes de acceso a datos de geolocalización o de cualquier índole.

3.4. Diferentes normas de conservación de datos han sido declaradas ilegales, se archivaron o enfrentan procesos de inconstitucionalidad

3.4.1. La directiva de retención de datos fue declarada ilegal en la Unión Europea

Este informe no puede dejar de mencionar que, en lo relativo a la retención y conservación de datos que propone el Decreto Legislativo, esta norma presenta los mismos problemas que presentaba la invalidada Directiva 2006/24 del Parlamento Europeo y del Consejo de la Unión sobre la conservación de datos generados o tratados en relación al servicio de comunicaciones electrónicas.[33] En el fallo que declara su invalidez, si bien se reconoce como legítimo el uso de datos y su preservación limitada para combatir delitos, se cuestiona fuertemente que las disposiciones no ofrecen suficiente claridad en su aplicación, lo que la torna en lesiva para los derechos fundamentales, especialmente el de la privacidad.

Al respecto, la Corte que declaró la invalidez de la Directiva cita en su sentencia algunas características necesarias en este tipo de normas y que estaban ausentes o apenas desarrolladas.[34] Algunas de estas características también están ausentes en el mecanismo de conservación propuesto por el Decreto Legislativo, como medidas que establezcan un rango razonable de vulneración no permanente (por espacio geográfico, grupos de personas vulnerables, etc.), la protección especial de sujetos cuyas comunicaciones requieran un nivel de protección más alto como el caso del secreto profesional y la redacción clara y detallada de todo el proceso de recolección y uso e inclusive el establecimiento de protocolos para garantizar la seguridad y posterior destrucción de los datos que ya no sean útiles.

Como es posible corroborar al comparar la Directiva Europea con el Decreto Legislativo 1182, este último no cumple con la mayoría de consideraciones señaladas por la Corte que declaró su invalidez. Por ende, el Decreto Legislativo 1182 adolece de los mismos problemas de legalidad que llevaron a la invalidez de la Directiva Europea de Conservación de Datos. Si bien el precedente de este organismo europeo no es vinculante para el Perú, los fundamentos allí expuestos revelan de forma clara el carácter lesivo que este tipo de normas tienen para la colectividad cuando no están bien diseñadas y no establecen con claridad sus verdaderos alcances y las acciones que mitigarán los posibles ejercicios abusivos.

3.4.2. El Proyecto de ley de retención de datos fue archivado en Paraguay

Un proyecto de ley que se discutió desde el año 2014 en Paraguay fue la "Ley que establece la obligación de conservar datos de tráfico,"[35] posteriormente conocida como ley "Pyrawebs." Este proyecto buscaba establecer la obligación de retención de tráfico relacionado con las telecomunicaciones de todos los habitantes del país sin excepción y su conservación por doce (12) meses con fines de investigación criminal.

Al respecto, más allá de los mecanismos que crean es interesante ver cómo este proyecto de ley cita dentro de su Exposición de Motivos el siguiente argumento para justificar su existencia:

> Teniendo en cuenta que la vida en el mundo se torna cada vez más insegura, la seguridad integral de las personas es de vital importancia y la sociedad necesita estar protegida; por ello el Estado debe cumplir con su obligación de brindar protección a la misma introduciendo normas legislativas tendientes a este fin.

A eso se añade también la justificación repetida (ya desvirtuada) de que 'solo' se conservarán datos de tráfico y no datos relativos al contenido de las comunicaciones electrónicas, para así no afectar el derecho al secreto de las comunicaciones. Además, este proyecto de ley también presentaba falencias conocidas como: falta de claridad en sus mecanismos de recolección, falta de garantías para evitar la sustracción de los datos tratados, ausencia de medidas destinadas a mitigar el impacto negativo en el derecho a la privacidad, entre otros.

Por estas razones, las cámaras legislativas de Paraguay decidieron finalmente archivar este proyecto. Al hacerlo, precisaron que no lo hacían en función a los objetivos que pretendía sino porque los mecanismos que planteaba excedían el equilibrio entre la búsqueda de seguridad ciudadana y orden público y la protección a los derechos a la privacidad, el secreto de las telecomunicaciones y la presunción de inocencia.

4. CONCLUSIONES

El objetivo de este informe es servir como un instrumento de análisis legal de los puntos más críticos del Decreto Legislativo 1182 referidos a sus motivaciones, mecanismos de acción y principales omisiones. En virtud de ello, se establecen algunas conclusiones a las que podemos llegar luego de este análisis.

Los datos de localización y geolocalización forman parte del contenido protegido por el derecho al secreto e inviolabilidad de las comunicaciones. Por tanto, su afectación solo debe darse atendiendo a los preceptos que señala la Constitución y, en la medida de lo aplicable, a las leyes de desarrollo existentes como las normas penales.

La afectación del secreto e inviolabilidad de las comunicaciones exige que exista un procedimiento bien definido y que la autorización sea dada por un juez que motive debidamente su decisión y apruebe las condiciones y el lapso de tiempo en que esta medida

será ejecutada. Esto se hace en respaldo a las garantías del debido proceso y la presunción de inocencia, condiciones necesarias para que un proceso no devenga en nulo.

Tal como lo han afirmado organizaciones internacionales como la ONU y la OEA, la retención y conservación de datos es una afectación gravísima contra el derecho de la privacidad. Los datos derivados de las comunicaciones son capaces de brindar mucha información acerca de una persona y su conservación masiva es injustificada, si el sujeto no está siendo investigado por un delito. Eso constituye una actuación estatal desproporcionada.

A la luz de precedentes como la invalidación de la Directiva Europea de retención de datos, el fallido paso del proyecto de ley de retención en Paraguay, entre otros, queda claro que si bien el objetivo bajo el cual se gestan este tipo de leyes es legítimo, los mecanismos destinados a implementar las acciones pueden no serlo, llevando a la creación de situaciones de abuso que perjudican derechos fundamentales, rompiendo así el equilibrio que debe existir entre afectación y satisfacción de derechos.

Visto todo esto, urge modificar el Decreto Legislativo 1182 en los extremos que (i) permite el acceso sin autorización judicial de la Policía a la ubicación de cualquier usuario de dispositivos móviles, y, (ii) ordena a las empresas de telecomunicaciones a conservar los datos derivados de las telecomunicaciones de sus usuarios por un período de tres años. ■

NOTAS

1 La localización por triangulación se obtiene registrando la intensidad de la señal que las diferentes torres reciben del dispositivo móvil del usuario. Este procedimiento es sencillo y fácil de implementar, además de que tiene diferentes niveles de exactitud dependiendo de la tecnología del operador y de la cantidad de torres cercanas al dispositivo móvil.

2 **Constitución Política del Perú, Artículo 2.—** Toda persona tiene derecho:
(…)
10. Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.
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. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.
Los documentos privados obtenidos con violación de este precepto no tienen efecto legal.
Los libros, comprobantes y documentos contables y administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación, salvo por orden judicial. (Énfasis agregado)

3 "En buena cuenta, este derecho prohíbe que las comunicaciones y documentos privados sean incautados, interceptados o intervenidos, salvo que exista una resolución judicial debidamente motivada que lo autorice. **Asimismo, garantiza que el contenido de las comunicaciones y documentos no sea difundido o revelado, así como la identidad de los participantes en el proceso de comunicación**. Lo que se prohíbe es toda injerencia arbitraria o abusiva en la vida privada de las personas, específicamente, en sus comunicaciones, independientemente de su contenido." (Énfasis agregado)
Voto individual del magistrado Mesía Ramirez en la Sentencia del Tribunal Constitucional emitida el 10 de enero de 2012 en el Expediente No. 03599-2010-PA/TC. URL: http://www.tc.gob.pe/jurisprudencia/2012/03599-2010-AA.html

4 Voto individual del magistrado Eto Cruz en la Sentencia del Tribunal Constitucional emitida el 10 de enero de 2012 en el Expediente No. 03599-2010-PA/TC. URL: http://www.tc.gob.pe/jurisprudencia/2012/03599-2010-AA.html

5 Sentencia del Tribunal Constitucional emitida el 27 de octubre de 2010 en el Expediente No. 00655-2010-PHC/TC. URL: http://www.tc.gob.pe/jurisprudencia/2010/00655-2010-HC.html

6 **Decreto Supremo No. 013-93-TCC, Texto Único Ordenado de la Ley General de Telecomunicaciones, Artículo 4.—** Toda persona tiene derecho a la inviolabilidad y al secreto de las telecomunicaciones. El Ministerio de Transportes, Comunicaciones, Vivienda y Construcción se encarga de proteger este derecho.

7 **Decreto Supremo No. 020-2007-MTC, Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, Artículo 13.—** Inviolabilidad y secreto de las telecomunicaciones
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**.
Las personas que en razón de su función tienen conocimiento o acceso al contenido de una comunicación cursada a través de los servicios públicos de telecomunicaciones, están obligadas a preservar la inviolabilidad y el secreto de la misma.
Los concesionarios de servicios públicos de telecomunicaciones están obligados a salvaguardar el secreto de las telecomunicaciones y la protección de datos personales, adoptar las medidas y procedimientos razonables para garantizar la inviolabilidad y el secreto de las comunicaciones cursadas a través de tales servicios, así como mantener la confidencialidad de la información personal relativa a sus usuarios que se obtenga en el curso de sus negocios, salvo consentimiento previo, expreso y por escrito de sus usuarios y demás partes involucradas o por mandato judicial.
Los titulares de servicios privados de telecomunicaciones deberán adoptar sus propias medidas de seguridad sobre inviolabilidad y secreto de las telecomunicaciones.
El Ministerio podrá emitir las disposiciones que sean necesarias para precisar los alcances del presente artículo. (Énfasis agregado)

8 **Resolución Ministerial No. 111-2009-MTC-03, Norma que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales, y regula las acciones de supervisión y control a cargo del Ministerio de Transportes y Comunicaciones.—**
6. ÁMBITO DE PROTECCIÓN
La protección del derecho a la inviolabilidad y al secreto de las telecomunicaciones y a la protección de datos personales, comprende, entre otros aspectos, los siguientes:
— El contenido de cualquier comunicación, de voz o de datos, cursado a través de las redes de telecomunicaciones u otros medios que la tecnología permita.
— Los mensajes de texto (SMS) y multimedia (MMS), entrantes y salientes.
— **El origen, destino, realización, curso o duración de una comunicación.**
— La información del tráfico de un abonado o usuario.
— Los datos codificados y decodificados de los registros de las llamadas.
— Los documentos, en soporte físico o magnético, y bases de datos que contengan la información referida anteriormente, así como aquellos que fueran elaborados para la prestación de los servicios públicos de distribución de radiodifusión por cable o de acceso a Internet.
— La información personal que los Operadores de Telecomunicaciones obtengan de sus abonados y usuarios en el curso de sus operaciones comerciales y que se encuentre contenida en soportes físicos, informáticos o similares, tales como documentos privados y bases de datos, en tanto el usuario o abonado no haya autorizado su difusión o esté permitida por el marco legal vigente.
— Los pagos, tales como el pago anticipado, pago a plazos y notificación de recibos pendientes, entre otros.
— La información referida al origen de la suspensión del servicio, distinto a la falta de pago, que hubiera motivado o generado la conexión o desconexión del servicio.
— Otros que se determine mediante Resolución Viceministerial.
Se exceptúa del ámbito de aplicación de la presente Norma, los supuestos previstos en la legislación vigente, referidos a cualquiera de los aspectos detallados en el presente numeral.

9 **Decreto Legislativo No 957, "Nuevo Código Procesal Penal", Artículo 230— Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles. —**
1. El Fiscal, 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 y la intervención sea absolutamente necesaria para proseguir las investigaciones, **podrá solicitar al Juez de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación.** Rige lo dispuesto en el numeral 4) del artículo 226 (…) (Énfasis agregado)

10 "22) La demandada, por otra parte, tampoco ha tenido en cuenta que en la forma como ha obtenido los elementos presuntamente incriminatorios, no solo ha vulnerado la reserva de las comunicaciones y la garantía de judicialidad, sino que ha convertido en inválidos dichos elementos. En efecto, **conforme lo establece la última parte del artículo 2°, inciso 10), de la Constitución, los documentos privados obtenidos con violación de los preceptos anteriormente señalados, no tienen efecto legal.** Ello, de momento, supone que por la forma como se han recabado los mensajes que han sido utilizados en el cuestionado proceso administrativo, su valor probatorio carece de todo efecto jurídico, siendo, por tanto, nulo el acto de despido en el que dicho proceso ha culminado. Se trata, pues, en el fondo, de garantizar que los medios de prueba ilícitamente obtenidos no permitan desnaturalizar los derechos de la persona ni, mucho menos, y como es evidente, que generen efectos en su perjuicio." (Énfasis agregado)
Sentencia del Tribunal Constitucional emitida el 18 de agosto de 2004 en el Expediente No. 1058-2004-AA/TC. URL: http://www.tc.gob.pe/jurisprudencia/2004/01058-2004-AA.html

11 "Artículo 259 .— Detención Policial
La Policía Nacional del Perú detiene, sin mandato judicial, a quien sorprenda en flagrante delito. Existe flagrancia cuando:
1. El agente es descubierto en la realización del hecho punible.
2. El agente acaba de cometer el hecho punible y es descubierto.
3. El agente ha huido y ha sido identificado durante o inmediatamente después de la perpetración del hecho punible, sea por el agraviado o por otra persona que haya presenciado el hecho, o por medio audiovisual, dispositivos o equipos con cuya tecnología se haya registrado su imagen, y es encontrado dentro de las veinticuatro (24) horas de producido el hecho punible. (Énfasis agregado)

12 El argumento contrario a este planteamiento es la afirmación de que en el momento de la redacción de estos artículos no era posible imaginar que la tecnología del futuro haría factible la obtención de datos de geolocalización en tiempo real que sirvieran a la investigación criminal y por lo tanto el supuesto de la flagrancia como presupuesto para autorizar la acción policial no se tuvo en cuenta. No obstante, aún si asumimos esto como cierto, los constituyentes sí podían prever la intervención de las comunicaciones o instrumentos de las líneas de telefonía fija en casos de flagrancia delictiva. ¿Por qué entonces no lo hicieron? La explicación más congruente es que la vulneración del secreto e inviolabilidad de las comunicaciones no solo resulta potencialmente más lesiva que cualquier otra sino que su realización requiere un concurso de actos complejos que justifican de sobra la existencia de un control judicial que limite los excesos que pudieran cometerse durante su ejecución.

13 "4. Según lo ha establecido este Tribunal en reiterada jurisprudencia, **la flagrancia en la comisión de un delito requiere el cumplimiento de cualquiera de los dos requisitos siguientes: a) la inmediatez temporal, es decir, que el delito se esté cometiendo o se haya cometido momentos antes; y, b) la inmediatez personal, es decir, que el presunto delincuente se encuentre en el lugar de los hechos, en el momento de la comisión del delito, y esté relacionado con el objeto o los instrumentos del delito.** (…)" (Énfasis agregado)
Sentencia del Tribunal Constitucional emitida el 14 de marzo de 2007 en el Expediente N.° 6142-2006-PHC/TC. URL: http://www.tc.gob.pe/jurisprudencia/2007/06142-2006-HC.html

14 "2. Que, por consiguiente y partiendo de la merituación de las pruebas obrantes en el expediente constitucional así como de las diligencias realizadas en el presente proceso, resultan plenamente acreditadas las aseveraciones efectuadas por la accionante de la presente causa respecto de los ciudadanos afectados en sus derechos, habida cuenta que (…) f) Que por tal motivo y reiterando los precedentes sentados con anterioridad, y a los cuales deben observancia obligatoria todos los jueces y tribunales de la República, conforme lo señala la Primera Disposición General de la Ley N.° 26435 –Ley Orgánica del Tribunal Constitucional, **este Tribunal ratifica que las variables de causalidad a los efectos de ejercer la potestad de detención, esto es, mandato judicial y flagrante delito, constituyen la regla general aplicable a todos los casos de detención, sea cual sea la naturaleza del ilícito cometido, de modo tal que las llamadas detenciones preventivas o detenciones sustentadas en la mera sospecha policial, carecen de toda validez o legitimidad constitucional** (…)" (Énfasis agregado) Sentencia del Tribunal Constitucional emitida el 19 de enero de 2001 en el Expediente N.° 1324-2000-HC/TC. URL: http://www.tc.gob.pe/jurisprudencia/2001/01324-2000-HC.html

15 LANDA, César. "El derecho fundamental al debido proceso y a la tutela jurisdiccional." En: Pensamiento Constitucional. Año VIII. No. 8. Lima: Pontificia Universidad Católica del Perú, 2002.

[16] **Código Procesal Penal, Artículo 230. - Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles**

1. El Fiscal, 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 y la intervención sea absolutamente necesaria para proseguir las investigaciones, podrá solicitar al Juez de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación. Rige lo dispuesto en el numeral 4) del artículo 226.
2. La orden judicial puede dirigirse contra el investigado o contra personas de las que cabe estimar fundadamente, en mérito a datos objetivos determinados que reciben o tramitan por cuenta del investigado determinadas comunicaciones, o que el investigado utiliza su comunicación.
3. El requerimiento del Fiscal y, en su caso, la resolución judicial que la autorice, deberá indicar el nombre y dirección del afectado por la medida si se conociera, así como, de ser posible, la identidad del teléfono u otro medio de comunicación o telecomunicación a intervenir, grabar o registrar. También indicará la forma de la interceptación, su alcance y su duración, al igual que la dependencia policial o Fiscalía que se encargará de la diligencia de intervención y grabación o registro. El Juez comunicará al Fiscal que solicitó la medida el mandato judicial de levantamiento del secreto de las comunicaciones. La comunicación a los concesionarios de servicios públicos de telecomunicaciones, a efectos de cautelar la reserva del caso, será mediante oficio y en dicho documento se transcribirá la parte concerniente.
4. Los concesionarios de servicios públicos de telecomunicaciones deben 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. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento.
5. Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, 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.
6. Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente
7. La interceptación no puede durar más de sesenta días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal y decisión motivada del Juez de la Investigación Preparatoria.

[17] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos (OEA) y Relatoría Especial de las Naciones Unidas (ONU) para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión. 21 de junio de 2013. URL: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927&lID=2

[18] **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.

[19] **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.

[20] **Pacto Internacional de Derechos Civiles y Políticos, Artículo 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.

21 Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos (OEA) y Relator Especial de las Naciones Unidas (ONU) para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión. 21 de junio de 2013. URL: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927&lID=2

22 Naciones Unidas. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. El Derecho a la Privacidad en la Era Digital. A/HRC/27/37. 30 de junio de 2014. Parrafo 19. URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_sp.doc

23 Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40. 17 de abril de 2013. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/06/PDF/G1313306.pdf?OpenElement

24 Naciones Unidas. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos El Derecho a la Privacidad en la Era Digital. A/HRC/27/37. 30 de junio de 2014. Párrafo 20. URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_sp.doc

25 Naciones Unidas. Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo. A/69/397. 23 de septiembre de 2014. Párrafo 55. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/22/PDF/N1454522.pdf?OpenElement

26 **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.

27 **Resolución de Consejo Directivo No. 138-2012-CD-OSIPTEL, Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, Articulo 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 (…)

28 Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relator Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de DDDHH y de los Pueblos (CADHP). 3 de mayo de 2015. URL: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=987&lID=2

29 "(…) La realidad actual nos demuestra que la naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.
Según los reportes de la DIVINCRI - PNP, en los últimos meses se ha incrementado la incidencia delictiva mediante la utilización de los equipos de comunicación de telefonía móvil. Las modalidades y mecanismos de operación, las organizaciones criminales y los lugares desde donde operan están plenamente identificados por la Policía Nacional del Perú, sin embargo, poco es lo que se puede hacer al respecto, dado que no se cuenta con el marco legal que favorezca la actuación policial no sólo para el combate y persecución de los delitos y faltas, sino sobre todo para la prevención de la ocurrencia de los mismos (…)
En ese marco, el objetivo principal de la captura y conservación de algunos datos es el de guardar por cierto tiempo el registro de sus comunicaciones, proscribiéndose el uso del presente mecanismo como una herramienta que pretenda regular el comportamiento de los usuarios y usuarias."

30 Anuario Estadístico 2014. Dirección Ejecutiva de Tecnologías Comunicación y Estadística. URL: https://www.pnp.gob.pe/documentos/ANUARIO%202014%20DIREST-PNP%20OK.pdf

31 "Durante el año 2014, la Policía Nacional del Perú registró, a nivel nacional, un total de 278,184 denuncias por comisión de los diferentes tipos de delitos, cifra que es superior en 10,166 casos más que el año anterior, representando un incremento de 3.79% en la incidencia delictiva. Por otra parte, se aprecia que en los delitos Contra el Patrimonio (Hurto, robo, apropiación ilícita, estafas, otros) se presentó la mayor cantidad de denuncias, registrándose un total de 185,015 denuncias que representa el 66.51% respecto al total nacional, seguido por los delitos Contra la Seguridad Publica (Peligro común, TID, Micro comercialización de drogas, Tenencia ilegal de armas, otros) con 40,016 denuncias que representa el 14.38%, en tercer término por los delitos Contra la Vida, Cuerpo y la Salud (Homicidios, aborto, lesiones, otros) con 27,582 denuncias y en cuarto lugar por los delitos Contra la Libertad (Personal, intimidad, domicilio, sexual, otros) con 13,536 denuncias (…)"

32 Resultados definitivos del III Censo Nacional de Comisarías 2014 realizado por el INEI. URL: http://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1254/index.html

33 Directiva 2006/24/CE del Parlamento Europeo del 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF

34 Tribunal Europeo de Justicia (Gran Sala). 8 de abril de 2014. Digital Rights Ireland Ltd e Irlanda. Comunicaciones electrónicas — Directiva 2006/24/CE — Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones — Conservación de datos generados o tratados en relación con la prestación de tales servicios — Validez — Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea. URL: http://curia.europa.eu/juris/document/document.jsf?docid=153045&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=ES&cid=225639

35 Ley "que establece la obligación de conservar datos de tráfico." URL: http://sil2py.diputados.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F102821