CONTRA EL

DL 1182

Decreto Legislativo 1182, Geolocalización y Proceso Penal

Sacrificio de garantías en favor de una supuesta eficacia investigativa

RICARDO ELÍAS PUELLES

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.

Ricardo Elías Puelles
Abogado titulado con mención sobresaliente por la Pontificia Universidad Católica del Perú. Cuenta con estudios de posgrado en Teoría del Delito (Universidad de Buenos Aires, Argentina), en Litigación Oral (Asociación Unidos por la Justicia, Argentina) y en Gestión de la Formación y Capacitación (Pontificia Universidad Católica del Perú). Formó parte de la I Escuela Latinoamericana de Defensores Penales (Instituto de Estudios Comparados en Ciencias Penales y Sociales, Argentina) y de la III Escuela de Verano en Ciencias Criminales y Dogmática Penal alemana (Georg-August Universität Göttingen, Alemania). Correo electrónico de contacto: ricardo@eliaspuelles.com

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

1. Los datos de localización y geolocalización pertenecen a los datos de transmisión de información y, al igual que los datos de contenido, se encuentran protegidos por los derechos fundamentales del secreto de las comunicaciones, intimidad y autodeterminación informativa.

2. El Decreto Legislativo 1182 establece un procedimiento de investigación policial que vulnera derechos fundamentales y que, en consecuencia, genera prueba prohibida que no podrá ser empleada en el proceso penal.

3. La flagrancia delictiva exige inmediatez temporal y personal para su configuración. En este sentido, el uso de dispositivos móviles o electrónicos no permiten la configuración de ninguno de los cuatro supuestos previstos en el artículo 259 del Código Procesal Penal por lo que jurídicamente no es posible su aplicación.

4. La aplicación del Decreto Legislativo no se restringe a delitos muy graves. La redacción amplía sus alcances a prácticamente cualquier delito del Código Penal.

5. El Decreto Legislativo restringe las funciones del Ministerio Público y confunde los roles de la Fiscalía con los de la Policía al conferirle tácitamente a esta última, la facultad de analizar jurídicamente y restringir derechos fundamentales.

6. El Decreto Legislativo no prevé qué sucederá con la información obtenida por la Policía cuando la Fiscalía no esté de acuerdo con la solicitud de acceso a la información relacionada a datos de localización y geolocalización o cuando el juez no convalide la medida requerida.

7. El Decreto Legislativo otorga el monopolio del procedimiento de obtención y tratamiento de datos de localización y geolocalización al Poder Ejecutivo, al establecer que el único contacto con las empresas operadores o de comunicaciones es una Unidad Especializada de la Policía.

8. El Decreto Legislativo no es compatible con los Arts. IV, VI, IX, 202, 203 y 230 del Código Procesal Penal.

1. INTRODUCCIÓN

No cabe duda que las nuevas tecnologías nos brindan numerosas posibilidades como la *interconexión* o el acceso a una fuente inagotable de *conocimiento*. No obstante, también viene gedo desafíos como el desarrollo de *nuevos delitos* (piénsese por ejemplo en la evolución de los delitos informáticos a la cibercriminalidad),[1] la facilidad para incrementar la comisión de graves delitos tradicionales como el narcotráfico[2] o el lavado de activos,[3] o el riesgo conte a nuestra *privacidad* y a la *protección de datos personales.*[4]

Sobre el último punto, invitamos al lector a responder las siguientes preguntas: ¿Qué dispositivo está empleando para leer este texto: un celular, una *tablet*, una laptop, una PC o lo tiene impreso?, ¿lleva consigo un celular?, ¿el celular está encendido?, ¿está conectado a una red WiFi?, ¿sabía que sus dispositivos pueden ser ubicados en cualquier momento y en cualquier lugar? Es decir, una persona, una empresa o el propio Estado podría saber dónde se encuentra exactamente usted mientras inicia esta lectura si es que está usando un aparato electrónico conectado a Internet. La reflexión que pretendemos iniciar gira sobre este punto: ¿la Policía, sin autorización judicial, puede estar facultada a acceder a información relacionada a nuestra geolocalización?, ¿cuáles pueden ser las consecuencias procesales de esta facultad? Antes de continuar, necesitamos desarrollar algunas ideas que nos acompañarán en el presente ensayo: (i) diferenciar entre datos de transmisión de información y datos de contenido; (ii) responder a qué categoría pertenecen los datos de geolocalización; y (iii) explicar cómo los datos de transmisión de información permiten la ubicación de dispositivos y personas a través de la geolocalización.

Este informe tiene por objeto analizar el Decreto Legislativo 1182 o "Decreto Legislativo que regula 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" (en adelante, el Decreto Legislativo) así como las consecuencias procesales que trae consigo al vulnerar derechos constitucionales sin autorización judicial previa.

2. CONCEPTOS PREVIOS

Cada vez que realizamos una llamada telefónica o videoconferencia, enviamos un mensaje de texto o un correo electrónico dejamos un *rastro* que puede ser observado y almacenado. Existe información relacionada al emisor, el receptor, la ubicación, el trayecto y el contenido de la comunicación. Si bien se reconoce que el contenido de la comunicación se encuentra protegido por el derecho al secreto de las comunicaciones, debemos tomar posición y reconocer que los datos de información también merecen esta protección. Para ello necesitamos diferenciar ambos conceptos y así evitar caer en confusiones terminológicas. De este modo, se entenderá por **datos de transmisión de información**, aquellos relativos a la información asociada a una comunicación que expresa el emisor, el destinatario y otros elementos como la hora del envío y la ubicación geográfica del creador del mensaje.[5] En cambio, nos referiremos a **datos de contenido** a aquellos relacionados con el mensaje o comunicación en sí mismo,[6] es decir a la información transmitida.

En este punto es necesario recordar que el artículo 1.d del Convenio de Budapest desarrolla el concepto de datos de transmisión de información bajo el rótulo **datos relativos al tráfico**, que define como: *"(…) datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente*". Tomando esta definición, coincidimos que se debe entender por **datos de geolocalización** a aquellos que, por sí mismos o debidamente tratados, son aptos para indicar la posición en el espacio de un objeto o de un sujeto con el que se vinculan, así como para trazar un perfil de sus desplazamientos.[7]

Más adelante explicaremos por qué los datos de transmisión de información (entre los que se encuentran los datos de geolocalización) sí se encuentran protegidos por el secreto de las comunicaciones, aunque en menor medida en comparación con el contenido o mensaje en sí mismo. Dicho de otro modo, el grado de protección es menor que a los datos de contenido pero eso no significa, en modo alguno, que se encuentren desprotegidos. Reconocer lo contrario significaría que cualquier persona o institución podría acceder a nuestra información, por lo que la convalidación judicial exigida por el Decreto Legislativo devendría en innecesaria.

Un aspecto que también debemos resaltar está relacionado al funcionamiento de la geolocalización en **cualquier equipo móvil**.[8] Así, cuando nos referimos a los sistemas que permiten identificar nuestra posición y el riesgo que ello representa,[9] debemos considerar qué tipo de sistemas existen y cómo funcionan. A fin de explicar cómo se relacionan los teléfonos móviles con la geolocalización, el Grupo de Trabajo sobre Protección de Datos de la Comunidad Europea advierte que:

> Durante todo el tiempo en que un dispositivo móvil permanece encendido, está en conexión permanente con una determinada estación base y el operador de telecomunicaciones lleva un registro continuo de estas conexiones. Cada estación de base tiene un número de identificación único y está registrada con una ubicación específica. Tanto el operador de telecomunicaciones como muchos dispositivos móviles son capaces de utilizar las señales de casillas (estaciones de base) solapadas para estimar la posición del dispositivo móvil con mayor precisión. Esta técnica también se denomina "triangulación."[10]

Pasemos a un ejemplo concreto. Para que no le pase nada a nuestra familia, un grupo de delincuentes nos exige el pago de una fuerte suma de dinero. Así, acabamos de recibir una llamada en nuestro celular desde un número fijo, luego desde un móvil, después recibimos un mensaje de texto, uno vía WhatsApp y otro a través de Facebook Messenger. Cada llamada o mensaje ha dejado un rastro digital y será labor del binomio Policía / Fiscalía organizar una investigación estratégica. De eso, no hay duda alguna. La pregunta es ¿la Policía o la Fiscalía necesitan autorización judicial previa para conocer el lugar desde donde se hicieron las llamadas o se enviaron los mensajes? Para el Ejecutivo, la respuesta es *no* pues únicamente se necesitaría la convalidación judicial posterior. Nosotros nos encontramos en la otra vía pues afirmamos que *sí* se requiere autorización judicial previa.

3. LA RESPUESTA DEL ESTADO PERUANO ANTE EL AUMENTO DE LA CRIMINALIDAD: AGILIZAR LA INVESTIGACIÓN CRIMINAL A COSTA DE NUESTRAS GARANTÍAS PROCESALES

3.1. La solicitud del Ejecutivo y el Debate en el Congreso

El aumento de la criminalidad en Perú generó que el 08 de junio de 2015 el Presidente de la República solicitase facultades extraordinarias para legislar en materia de seguridad ciudadana. En este sentido, el Proyecto de Ley No. 4569-2014/PE propuso siete materias de delegación legislativa, entre las que se encontraba potenciar la capacidad operativa, organización, el servicio policial y régimen disciplinario de la Policía Nacional. Esta fue la delegación que justificó la aprobar una norma que creaba la facultad policial de ubicar dispositivos electrónicos sin conocimiento previo del Ministerio Público y sin autorización judicial. Pese a lo cuestionable de esta propuesta, no fue mencionada en la exposición de motivos del proyecto de ley que solicitaba facultades legislativas.[11]

El jueves 18 de junio de 2015, el Presidente del Consejo de Ministros y los titulares del Ministerio del Interior, José Luis Pérez Guadalupe, y del Ministerio de Justicia y Derechos Humanos, Gustavo Adrianzén, acudieron al Congreso a exponer y defender el proyecto de ley antes referido. El Ministro Pérez Guadalupe después de señalar que "solo el 40% de los internos de los establecimientos penales han cometido delitos contra el patrimonio, pero este 40% genera prácticamente el 100% de la inseguridad ciudadana,"[12] sentencia que hacen falta herramientas que le permita enfrentar, entre otros, el sicariato, la extorsión y el llamado "raqueteo." Una de estas herramientas, para él, será que la Policía cuente con la posibilidad de solicitar y obtener sin autorización judicial información relacionada a los datos de transmisión de información.

Durante el debate, se cuestionó la facultad policial trayendo a colación las experiencias de la Dirección Nacional de Inteligencia en los siguientes términos: "¿quién nos garantiza que este aparato no va a servir para otros fines si usted no tiene al fiscal, si usted no tiene al juez? Lamentablemente hemos tenido la terrible experiencia de la DINI."[13] Asimismo, se añadió

> ¿Qué confianza vamos a tener para que la famosa geolocalización no se use con fines de persecución política? Allí tienen que haber una autoridad que no sea solo Policía, tiene que haber una autoridad judicial, un fiscal y el ministro nos ha dicho no, mientras llamamos al fiscal, ya todo, ya se fue la persona, no, pero se establece mecanismos, la Dirandro tiene mecanismo con los cuales hace operaciones con autorizaciones incluso de jueces (…) Entonces, tendrá que verse la manera pues, de que haya fiscales, que estén sentados allí, permanentemente asumiendo la responsabilidad judicial del tema, porque no puede ser solamente manejado por una autoridad sin la vigilancia de otra autoridad.[14]

El Ministro Pérez Guadalupe respondió estos válidos cuestionamientos señalando que (i) se aplicaría únicamente en casos de flagrancia a fin de dotar de eficacia la investigación criminal,[15] y, (ii) que no vulnera el secreto de las comunicaciones.[16] Pese a los argumentos

esgrimidos en la Sesión, diez días después de la presentación del Proyecto de Ley, en Pleno Extraordinario del Congreso de la República ,no sólo se aprobó el pedido del Ejecutivo sino que se acordó exonerarlo de una segunda votación. Así, a través de la Ley No. 30336, el Congreso dio luz verde al Ejecutivo para legislar, entre otros, en procedimientos especiales para la investigación criminal.

3.2. El Decreto Legislativo 1182

El "Decreto Legislativo que regula 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" fue publicado el 27 de julio de 2015. En las siguientes líneas analizaremos los alcances de esta norma y los problemas procesales que, a nuestro entender, genera.

3.2.1. La "prevención" no puede ser considerada como uno de los objetivos del Decreto Legislativo 1182 y, por tanto, debe ser excluida

El primer punto de reflexión gira en torno al artículo 1 del Decreto Legislativo pues precisa que el objeto de la norma es "*fortalecer las acciones de prevención, investigación y combate de la delincuencia y el crimen organizado, a través del uso de tecnologías de la información y comunicaciones por parte de la Policía Nacional del Perú.*" Debemos preguntarnos ¿por qué la Policía debe estar facultada a solicitar información relacionada a la geolocalización, sin autorización judicial, a fin de prevenir la comisión de futuros delitos? Si se solicitó esta facultad legislativa extraordinaria fue, a decir del Ejecutivo, para fortalecer la investigación y el combate de la delincuencia y el crimen organizado, mas no para realizar acciones preventivas ya que en este caso, ninguno de los supuestos previstos en el artículo 3 de la misma norma lo posibilita.

El lector debe saber que existen *softwares* y algoritmos que están siendo desarrollados a través del uso de datos provistos por las compañías telefónicas –como los de localización y de geolocalización– con los que se trata de prevenir la comisión de delitos.[17] Toda vez que las acciones de *prevención*[18] vinculados a la obtención de datos de transmisión de información se acercan a las labores de inteligencia y se alejan de las de investigación criminal, deberían ser derogadas del alcance de esta norma. De ser estrictamente necesario, éstas deberían de ser debatidas y reguladas por una normal especial donde se establezcan sus requisitos y límites.

3.2.2.El Decreto Legislativo afecta derechos fundamentales

El artículo 6 del Decreto Legislativo precisa que se "*excluyen expresamente cualquier tipo de intervención de las telecomunicaciones, las que se rigen por los procedimientos correspondientes.*" Con esto, el Ejecutivo trata de evitar cuestionamientos relacionados a la restricción de derechos fundamentales en la búsqueda y obtención de medios de pruebas. Sin embargo, consideramos que sí se afectan tanto el derecho al secreto de las comunicaciones (artículo 2.10 Const.), a la intimidad (artículo 2.7 Const.) como a la autodeterminación informativa (artículo 2.6 Const.). Pese a que el objetivo de este artículo no es realizar un análisis

constitucional de los derechos fundamentales afectados, sí es necesario advertir que el Estado, al ordenar que se efectúe una **audiencia de convalidación** de la facultad policial, reconoce que se están afectando derechos fundamentales pues, de lo contrario, esta diligencia sería innecesaria.

En primer lugar, no debemos olvidar que con las nuevas tecnologías lo que se transmite no sólo es el contenido (mensaje) sino también información relacionada al emisor, sea de manera consciente o inconsciente. Así, como advertíamos al inicio, cada llamada o mensaje que enviamos a través de las redes móviles o las nuevas tecnologías está compuesta por datos de información de la transmisión y de contenido. Si se justifica realizar un trato diferenciado entre ambas pues la exigencia será mucho mayor en el caso de una intervención telefónica y menor cuando se requiera la ubicación del dispositivo. Esto no justifica excluir de su protección a una de ellas[19] más aún cuando el Tribunal Constitucional,[20] la Corte Interamericana de Derechos Humanos en el Caso Escher y otros vs. Brasil,[21] y el Tribunal Europeo de Derechos Humanos[22] así lo han reconocido.

En segundo lugar, consideramos que se afecta la intimidad por cuanto todas las personas tienen el derecho a defenderse de la divulgación de hechos privados.[23] En un mundo globalizado e interconectado como el nuestro, ¿acaso no tenemos el derecho a mantener en reserva el lugar donde nos encontramos o los que hemos visitado e, incluso, por dónde hemos deambulado? Piense el lector el trayecto que ha tenido el día de hoy, esta semana, este mes o este año, los lugares o las personas a las que visitó o con quienes se reunió: ¿usted está de acuerdo que la Policía puede solicitar esta información sin autorización judicial? Este Decreto Legislativo no sólo permite localizarnos en tiempo real sino acceder a nuestra localización histórica y monitorear nuestro desplazamiento futuro.

En tercer lugar, consideramos que en gran medida también afecta el derecho a la autodeterminación informativa,[24] ya que deberían ser los titulares de las líneas telefónicas quienes autoricen la ubicación de sus equipos telefónicos o, en todo caso, el juez a través de una resolución debidamente motivada. En este sentido, Caro Coria recuerda que:

> (…) si bien la norma señala que éste procedimiento se aplicará en los casos de flagrancia, y se trata de una intervención de los equipos, la norma no dice nada sobre los titulares de los equipos, quienes en realidad son los afectados directos con la intervención a sus equipos; y quienes por lo menos deberían tener la calidad de investigados para poder dictarse dicha medida contra sus equipos.[25]

A partir de este breve análisis, ponemos en evidencia que sí existen afectaciones a derechos fundamentales que exigen una autorización judicial previa. El artículo 6 del Decreto Legislativo trata de sostener lo contrario pero la doctrina y jurisprudencia es clara al respaldar nuestra posición.

3.2.3. Análisis de los supuestos de procedencia: flagrancia delictiva, pena mayor a cuatro años y necesidad de la medida

En las líneas siguientes, trataremos de demostrar que es imposible jurídicamente que nos encontremos ante supuestos de flagrancia que habiliten la geolocalización del presunto agente, ya que dicha figura requiere dos elementos: inmediatez temporal e inmediatez personal. Este último no se encuentra presente en los delitos cometidos a través de dispositivos móviles o similares. Prescindir de la inmediatez personal ampliaría peligrosamente la figura de flagrancia delictiva. Por otro lado, el Decreto Legislativo no restringe la geolocalización a casos de extorsión, trata de personas u otros delitos muy graves como fue plantead inicialmente, sino virtualmente a todo tipo de delitos previstos en el Código Penal. Además, el Decreto Legislativo exige que sea el Policía y no el Fiscal quien evalúe la *necesidad,* subprincipio que integra el principio de proporcionalidad, de restringir un derecho fundamental; es decir, propicia la confusión jurídica de roles.

En primer lugar, **la única posibilidad de aplicar el Decreto Legislativo es eliminando (peligrosamente) la inmediatez personal como requisito de la flagrancia delictiva**. En efecto, respecto al primer requisito, el Tribunal Constitucional ha establecido que de manera copulativa y no disyuntiva debe de reunirse criterios de inmediatez temporal y personal para su aplicación. De esta forma, el Supremo Intérprete en los pronunciamientos más recientes[26] ha establecido:

> (…) que la flagrancia en la comisión de un delito presenta la concurrencia de dos requisitos insustituibles: a) la inmediatez temporal, es decir, que el delito se esté cometiendo o que se haya cometido 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, ofreciendo una prueba evidente de su participación en el hecho delictivo."[27]

Al analizar los cuatro supuestos de flagrancia previstos en el artículo 259 del Código Procesal Penal caemos en cuenta que estos no cobijan aquellos casos para los que el Decreto Legislativo fue promulgado. Imaginemos que acabamos de recibir una llamada exigiéndonos un monto de dinero para que nuestro negocio no sea incendiado. La pregunta es: ¿en cuál de los cuatro supuestos de flagrancia nos encontramos: flagrancia clásica, cuasi-flagrancia, flagrancia por indicios o presunción de flagrancia?

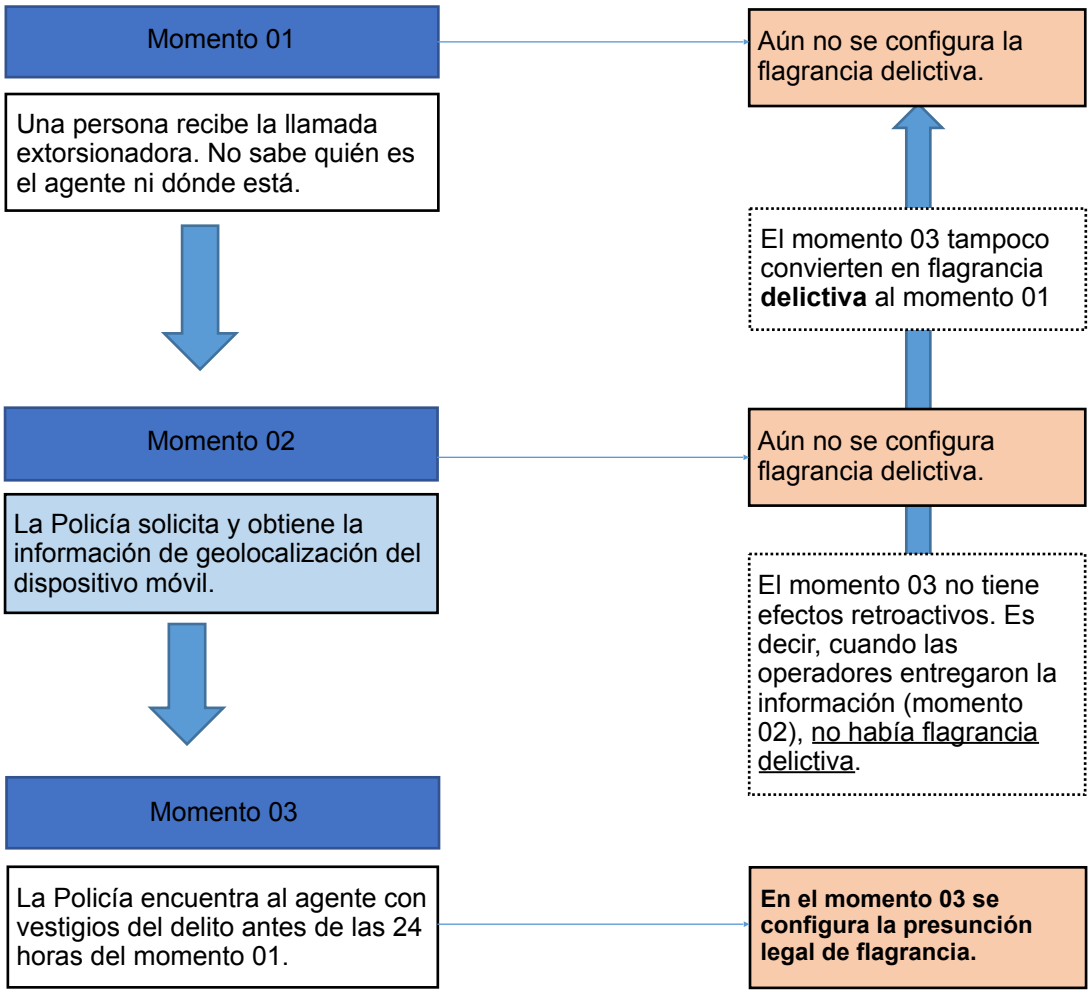
a) No nos encontramos frente a la flagrancia clásica o flagrancia propiamente dicha pues el agente no ha sido descubierto mientras está realizando el hecho punible. Es más, no sabemos quién es este mientras se lleva a cabo la llamada.

b) El agente tampoco ha sido descubierto después de la realización del hecho punible. Nuevamente, lo que el binomio Policía / Fiscalía deben hacer es identificar al responsable del delito pero la mera recepción de la llamada –o mensaje de texto, WhatsApp, etc.– no posibilita en sí su descubrimiento. Este es un círculo vicioso pues para emplear la geolocalización del dispositivo necesitaríamos haber localizado previamente al agente pues, de lo contrato, el agente no habría sido descubierto y, por lo tanto, no nos encontraríamos en un supuesto de flagrancia.

c) Ni el agraviado ni otra persona y mucho menos un dispositivo audiovisual han identificado al agente durante o inmediatamente después de la comisión del hecho delictivo. En consecuencia, no nos encontramos ante este supuesto de flagrancia por indicios.

d) Finalmente, la presunción legal de flagrancia tampoco se da ya que el agente no ha sido *encontrado* con vestigios de la comisión del delito. Este supuesto se aplica cuando el agente ya fue identificado y ubicado por la Policía y, por tanto, puede ser detenido. En el caso de la geolocalización, no podemos decir que se *encontró* al agente sino que *podría ser encontrado* si se accede a la ubicación del dispositivo y eso no es flagrancia.

Trataremos de ser gráficos para demostrar que recién estaremos en flagrancia si se encuentra al agente con vestigios del delito. Esto significa que cuando la Policía solicita la geolocalización aún no se encuentra en flagrancia ya que la figura procesal no puede legitimar acciones anteriores a su configuración.



La geolocalización sí permitiría encontrar al agente, incluso, dentro de las 24 horas de su comisión pero no por encontrarnos en un supuesto de flagrancia sino ante la comisión de un delito que merece ser investigado a través de búsqueda de pruebas con restricción de derechos, lo cual –como más adelante demostraremos– requiere autorización judicial previa. Considerar que nos encontramos ante un delito flagrante sería restringir esta categoría procesal a la inmediatez temporal y prescindir de la inmediatez personal. Ello, sin duda, sería relajar las garantías procesales de todo ciudadano. Si queremos invocar casuística, debemos tener presente que de acuerdo a lo reportado por la Policía Nacional, el primer caso de empleo de geolocalización ante un (imposible) flagrante delito se trató de un "auto secuestro."[28] El secuestro era una farsa. En consecuencia, tanto la Policía que solicitó y accedió como la operadora que brindó información, lesionaron derechos fundamentales de un ciudadano.[29]

Nuestra intención en este punto es únicamente dejar abierta la discusión en torno a los alcances de la flagrancia en una sociedad en la que se va incrementado la comisión de delitos a través de las nuevas tecnologías. Ello nos llevará a reflexionar sobre el requisito de inmediatez personal en los casos de flagrancia de este tipo de delitos. Sin embargo, nuestra posición es que no debemos permitir dicha flexibilización, ya que el riesgo para los ciudadanos es mayor al de la eficacia investigativa.

En segundo lugar, el Ejecutivo planteó la facultad legislativa como una propuesta excepcional para combatir casos de sicariato, extorsión, tráfico ilícito de drogas e insumos químicos, usurpación, tráfico de terrenos y tala ilegal de madera pero **la redacción del Decreto Legislativo permite solicitar la geolocalización, sin autorización judicial, de prácticamente cualquier delito previsto en el Código Penal**. Si concordamos el artículo 6.2 con el artículo 1 del Decreto Legislativo tenemos que esta norma se aplica tanto a la delincuencia común como al crimen organizado; es decir, a todo el catálogo de delitos del Código Penal. En vez de seleccionar un grupo específico de delitos en los que se podría aplicar la geolocalización, como el en caso de la interferencia de las comunicaciones, el Ejecutivo aprobó que sea aplicable a todos los ilícitos sancionados con pena superior a cuatro años de privación de libertad.

De este modo, los delitos que posibilitan la geolocalización sin autorización judicial no se reducen a aquellos catalogados como graves[30] pues esta herramienta también podría emplearse ante casos de estafa, corrupción de funcionarios, fraude informático, fraude en la administración de personas jurídicas, ultraje a los símbolos patrios, y un largo etcétera.[31] Como puede apreciarse, al no existir una clara restricción, posibilita la ubicación en tiempo real de cualquier ciudadano que cuente con un dispositivo electrónico y que haya sido denunciado ante la Policía.

En tercer lugar, **la norma exige que el acceso a los datos constituya un medio necesario para la investigación**. Este extremo está relacionado con el *subprincipio de necesidad* que forma parte del *principio constitucional de proporcionalidad*, exigido cuando se deben adoptar acciones que restringen derechos fundamentales. Siendo esto así, nos debemos preguntar: ¿a quién le corresponde realizar el análisis jurídico constitucional para la restricción de derechos en la búsqueda de pruebas? ¿A la Policía o a la Fiscalía? Recordemos

que es la Constitución la que posibilita excepcionalmente que la Policía pueda realizar este tipo de actos pero únicamente en dos casos concretos: detención (artículo 2.24.f Const.) y allanamiento (artículo 2.9 Const.). De esta manera, para la afectación al secreto de las comunicaciones, se requiere autorización judicial previa. El Decreto Legislativo no puede legitimar una restricción constitucional tan grave.

3.2.4. Un procedimiento inconstitucional que merma la función del Fiscal en el conocimiento e investigación del delito

Los artículos 4 y 5 del Decreto Legislativo regulan el procedimiento policial para acceder a la ubicación de los dispositivos electrónicos y el pedido de convalidación judicial. A continuación analizaremos los pasos que sigue este procedimiento especial y demostraremos que existen vicios que corroboran nuestra posición: el sacrificio de garantías en aras de una supuesta eficacia investigativa.

a) *La unidad a cargo de la investigación policial, una vez verificados los supuestos del artículo precedente, pone en conocimiento del Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la Policía Nacional del Perú para efectos de la localización o geolocalización* (artículo 4.1). La norma condiciona la puesta en conocimiento de los hechos denunciados a una previa verificación a cargo de la Policía de los supuestos que analizamos en el apartado anterior y que, como vimos, impide tratar los delitos cometidos a través de dispositivos móviles bajo la figura de flagrancia delictiva. Dicho de otro modo, la redacción es tendenciosa pues, de acuerdo al artículo 331.1 del Código Procesal Penal,[32] la Policía debe de comunicar inmediatamente la denuncia formulada por un ciudadano ante su dependencia y no condicionarlo a la verificación previa de los referidos supuestos.

b) *La unidad especializada de la Policía Nacional del Perú que recibe el requerimiento, previa verificación del responsable de la unidad solicitante, cursa el pedido a los concesionarios de los servicios públicos de telecomunicaciones o a entidades públicas relacionadas con este servicio, a través del correo electrónico institucional u otro medio idóneo convenido* (artículo 4.2). Ya hemos esgrimido los argumentos por los que la Policía no tiene la facultad constitucional de solicitar datos de localización o geolocalización a las empresas de comunicación al encontrarse protegidas por el derecho fundamental del secreto de las comunicaciones. No hemos tenido acceso al protocolo que regula el procedimiento que estamos analizando; sin embargo, la Policía ya está haciendo uso de esta facultad. Esperamos que todo el circuito de comunicación -desde el registro de la denuncia, la comunicación al Ministerio Público así como a la Unidad Especializada, la verificación del responsable hasta los correos electrónicos de solicitud y de respuesta de las operadoras- se encuentre anexo a la carpeta fiscal pues, de lo contrario, se estaría restringiendo el derecho a la defensa ya que no tendría la posibilidad de verificar cómo se desarrolló el procedimiento.

c) L*os concesionarios o servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata, las veinticuatro (24) horas del día de los trescientos*

sesenta y cinco (365) días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento (artículo 4.3). Consideramos que el término "inmediato" aumenta los riesgos al condicionar la aplicación de esta facultad excepcional a casos de flagrancia. Imaginemos que el 1 de enero de 2016 a las 00:00 recibimos una llamada extorsionadora. Acudimos a la Policía a las 18:00, mientras se realizan las comunicaciones respectivas pasan algunas horas y la Unidad Especializada remite la comunicación a la operadora a las 23:00 y esta responde a las 01:00. A quienes aún consideren que sólo se requiere inmediatez temporal y no personal para la configuración de la flagrancia, les preguntamos ¿qué harían con la información recibida pues aún cuando encontrasen al agente? Al haber pasado más de 24 horas, este no podrías detenido. Es más, habrían recibido la información cuando la flagrancia (que consideramos no se configura) ya habría cesado.

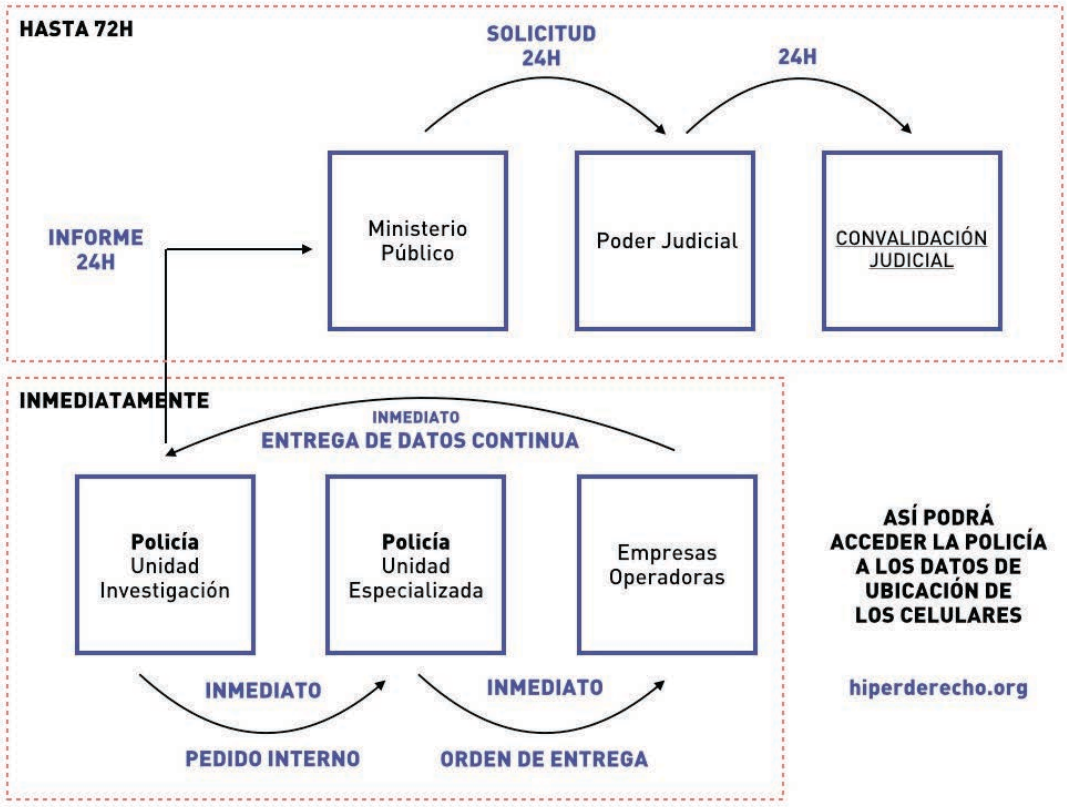
d) *La unidad a cargo de la investigación policial realiza las diligencias pertinentes en consideración de la información obtenida y a otras técnicas de investigación, sin perjuicio de lo establecido en el artículo 5* (artículo 4.4). Que la Policía realice actos de investigación no genera problema alguno, pues forman parte de sus funciones conforme se encuentra previsto en el artículo 67 del Código Procesal Penal. Nuestra crítica se dirige a que, salvo detención policial o allanamiento en flagrancia, no está facultada constitucionalmente a restringir nuestro derecho al secreto de las comunicaciones.

e) *La unidad policial a cargo de la investigación policial, dentro de las 24 horas de comunicado el hecho al Fiscal correspondiente, le remitirá un informe que sustente el requerimiento para su convalidación judicial* (artículo 5.1). *El Fiscal dentro de las veinticuatro (24) horas de recibido el informe, solicita al Juez la convalidación de la medida* (artículo 5.2). La redacción es inadecuada y sugiere que en todos los casos el Fiscal solicitará la convalidación judicial. Entendemos que no es así pues, nuevamente, el titular de la acción penal es el Fiscal y, de acuerdo al artículo 60.2 del Código Procesal Penal: "El Fiscal conduce desde su inicio la investigación del delito. Con tal propósito la Policía Nacional está obligada a cumplir los mandatos del Ministerio Público en el ámbito de su función." En consecuencia, pese a que la norma no lo expresa, si el Fiscal no está de acuerdo con la solicitud de la Policía tiene toda la potestad de ordenar se deje sin efecto la medida. El problema surgirá cuando la Policía haya obtenido información relacionada a la localización o geolocalización y después la Fiscalía muestre su disconformidad con tal pedido: ¿qué sucede con la información?, ¿quién se responsabilizará por la lesión sufrida por el ciudadano afectado?. Al no contar con el Protocolo de actuación (porque el Ejecutivo le ha conferido la condición de información reservada) no sabemos de qué forma la Fiscalía comunicaría la revocatoria de la solicitud policial a la operadora de telefonía: ¿directamente?, ¿a través de la Unidad Especializada de la Policía?, ¿a través de la Unidad de Investigación?

f) *El juez competente resolverá mediante trámite reservado y de manera inmediata, teniendo a la vista los recaudos del requerimiento fiscal, en un plazo no mayor de 24 horas. La denegación del requerimiento deja sin efecto la medida y podrá ser apelada por el Fiscal.*

El recurso ante el juez superior se resolverá en el mismo plazo y sin trámite alguno (artículo 5.3). *El juez que convalida la medida establecerá un plazo máximo que no excederá de sesenta (60) días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal* (artículo 5.4). Consideramos que este último paso debió ser el segundo en el procedimiento –el primero, obviamente, sería la comunicación y solicitud a cargo del Fiscal–. Ya que toda norma es perfectible, consideramos que en una eventual reforma, debería establecerse, al igual que en artículo 230 del Código Procesal Penal, que la resolución judicial debería indicar la información a la cual la Fiscalía puede acceder. Esto impedirá que la convalidación judicial sea tomada como un "cheque en blanco" que autoriza cualquier solicitud de información relacionada a la localización. Sin esta precisión, la Fiscalía o la Policía podrían solicitar ubicaciones históricas que no se encuentran vinculadas a la investigación criminal y, de este modo, lesionar el derecho a la intimidad personal. Imagine que se accede a la siguiente información: el móvil todos los domingos de los últimos dos meses acude entre las 09 y las 10 a una mezquita, todas las tardes de lunes a viernes a un hospital, todas las noches a un centro de rehabilitación para consumidores de drogas. Aun cuando parece ficción, esta información es accesible. De ahí que sea necesario el control judicial previo, no sólo para autorizar el acceso a información vinculada a la localización y geolocalización sino también a los alcances de esta medida. Consideramos que la norma no establece forma alguna, a través de la cual, el Ministerio Público o el Poder Judicial informen a las operadoras móviles la denegatoria del pedido de localización o geolocalización o su no convalidación judicial. Esto debió ser incluido para no dejar en manos de la Policía el monopolio de nuestra información.

El siguiente flujograma explica gráficamente los pasos que, de acuerdo al Decreto Legislativo, sigue la Policía para acceder a nuestra localización o geolocalización.



Luego de analizar este flujograma, nos preguntamos: ¿qué pasa si la persona afectada acude directamente al Ministerio Público a denunciar, por ejemplo, una extorsión telefónica? Al no encontrarse acreditada o regulada normativamente, ¿la Fiscalía debería derivar el caso a la Unidad de Investigación Policial para que solicite, a su vez, que la Unidad Especializada de la Policía requiera a las empresas operadoras la ubicación del dispositivo electrónico? Si esto es así, el procedimiento estaría siendo monopolizado por el Ejecutivo, a través de la Policía, desplazando a su vez al titular natural de la acción penal.

3.2.5. Modificación de tipos penales

Es importante advertir que el correlato a la flexibilización de la figura de flagrancia delictiva y la afectación injustificada del secreto de las comunicaciones fue el endurecimiento del ordenamiento punitivo a través de la elevación de sanciones penales e inclusión de nuevos supuestos típicos. Este hecho es relevante por cuanto la política criminal adoptada por el gobierno (en lo sustantivo y procesal) nos permite afirmar que se están siguiendo lineamientos propios de un **Derecho Penal del Enemigo**.[33] Como veremos en el próximo apartado, el Decreto Legislativo es contrario a las garantías y principios contenidos en el Código Procesal Penal.

Variación	C. Penal	Delito	Comentario
Modifica	Artículo 162	Interferencia telefónica	Eleva la sanción máxima del tipo base de 06 a 10 años. Las agravantes se elevan de 10 a 15 años.
Incorpora	Artículo 162-A	Posesión o comercialización de equipos destinados a la interceptación telefónica o similar	Incorpora este nuevo delito; sin embargo, su redacción complica la probanza pues no basta la posesión o comercialización de los equipos sino que se exige que el destino de su uso sea el de interceptar ilegalmente las comunicaciones.
Modifica	Artículo 222-A	Penalización de la clonación o adulteración de terminales de telecomunicaciones	Eleva la sanción máxima de 05 a 06 años de pena privativa de libertad. Además, agrega el IMEI electrónico o físico como objeto de protección de la clonación o adulteración.
Modifica	Artículo 368-A	Ingreso indebido de equipos o sistema de comunicación, fotografía y/o filmación en centros de detención o reclusión	Incorpora una nueva conducta reprochable: proporcionar la señal de WiFi del exterior para permitir el acceso a internet de los internos.

4. EL DECRETO LEGISLATIVO 1182 ES CONTRARIO AL CÓDIGO PROCESAL PENAL

Si bien el Decreto Legislativo le otorga a la Policía una facultad "especial" de investigación, lo cierto es que ésta pertenece a la fase de *diligencias preliminares* y como tal debe respetar los parámetros previstos en el Código Procesal Penal. Afirmar lo contrario, sería reconocer que nos encontramos ante un procedimiento policial ajeno al proceso penal. Siendo esto así:

4.1. El Decreto Legislativo genera confusión de roles entre la Policía y el Ministerio Público

De acuerdo al artículo IV del Código Procesal Penal, el Ministerio Público es el titular del ejercicio público de la acción penal y el encargado de conducir la investigación criminal desde el inicio. En consecuencia, "*conduce y controla jurídicamente los actos de investigación que realiza la Policía Nacional.*" Como analizamos anteriormente, el Decreto Legislativo fue diseñado para que el pedido de información relacionado a la localización y geolocalización estuviese en control y monopolio del Poder Ejecutivo, a través de la Policía Nacional. Así, al realizarse un acto de investigación que restringe derechos fundamentales, sin conocimiento previo del Ministerio Público y sin autorización judicial, se vulnera el artículo bajo análisis.

Un problema adicional que el Decreto Legislativo genera es la confusión de roles en la investigación criminal. Así, un logro obtenido con el Código Procesal Penal fue circunscribir las funciones de la Policía al plano operativo / forense y las funciones de la Fiscalía al plano jurídico. Antes de la promulgación del referido Código, por ejemplo, la Policía tenía la facultad de calificar jurídicamente los hechos investigados bajo las figuras de atestado policial y parte policial. El primero se refiere a la calificación jurídica y atribución de responsabilidad al investigado, mientras que la segunda al reconocimiento contrario, es decir, a la falta de responsabilidad.

Sostenemos que el Decreto Legislativo renueva esta confusión al exigir que sea el Policía y no el Fiscal quien valore jurídicamente si nos encontramos ante un supuesto de flagrancia de cualquier delito que sea sancionado con más de cuatro años en el Código Penal (recordemos que el Ejecutivo no incorporó una lista taxativa de aplicación, sino empleó una fórmula general que no distingue entre tipos de delitos). Si a esto agregamos la discusión jurídica que existe respecto al alcance de la flagrancia como institución procesal, el panorama resulta mucho más sombrío.

4.2. La solicitud de datos relacionados a la localización y geolocalización se enmarcan dentro del catálogo de búsqueda de pruebas con restricción de derechos

El Decreto Legislativo le confiere el carácter de jurisdiccionalidad a un acto policial. Este hecho vulnera el numeral 3 del artículo IV del Código Procesal, el cual prevé que los actos de investigación que practica el Ministerio Público o la Policía Nacional no tienen carácter jurisdiccional. Al respecto, señala que cuando una decisión de esta naturaleza sea indispensable tendrá que ser solicitada al órgano jurisdiccional. Como hemos expuesto hasta este punto, se requiere de autorización judicial previa para acceder a los datos de localización y geolocalización de dispositivos móviles por cuanto estos pertenecen a un titular (a una persona) cuyos derechos al secreto de las comunicaciones, a la intimidad y a la autodeterminación informativa se encuentran protegidos constitucionalmente.

En esta misma línea, de acuerdo al artículo VI del Código Procesal Penal, la actuación policial prevista por el Decreto Legislativo es ilegal toda vez que:

> Las medidas que limitan derechos fundamentales, salvo las excepciones previstas en la Constitución, sólo podrán dictarse por la autoridad judicial, en

> el modo, forma y con las garantías previstas por la Ley. Se impondrán mediante resolución motivada, a iniciativa de la parte procesal legitimada. La orden judicial debe sustentarse en suficientes elementos de convicción, en atención a la naturaleza y finalidad de la medida y al derecho fundamental objeto de limitación, así como respetar el principio de proporcionalidad.

Recordemos que los únicos supuestos en los que la Policía se encuentra facultada para restringir derechos fundamentales sin autorización judicial son: detención (artículo 2.24.f de la Constitución) y allanamiento (artículo 2.9 de la Constitución). En todos los demás casos, se requerirá resolución judicial motivada y que respete el principio de proporcionalidad constitucional.

Aunado a este punto, toda vez que la obtención de datos de transmisión de la información constituye una diligencia de búsqueda de pruebas con restricción de derechos, son aplicables los preceptos generales del Capítulo I del Título III del Código Procesal Penal. Dichas normas exigen un pronunciamiento judicial previo a la restricción del derecho, el cual debe estar debidamente motivado y respetar el principio de proporcionalidad.

Recordemos en este punto que el artículo 230 del Código Procesal Penal regula la intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles. Así, el numeral 4 de la norma en referencia precisa 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, 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.

Como puede apreciarse, un mismo supuesto de hecho (el acceso a la geolocalización de teléfonos móviles) ahora reviste dos mecanismos procesales: uno constitucional –exige resolución judicial previa– y uno inconstitucional –permite el acceso sin resolución judicial previa–. Como hemos anotado anteriormente, la flagrancia no valida el empleo del Decreto Legislativo.[34]

4.3. Los medios de prueba obtenidos a través del Decreto Legislativo generan prueba prohibida

Al lesionar derechos fundamentales, la facultad policial extraordinaria bajo análisis trae consigo la ilegitimidad de la prueba obtenida. En efecto, los numerales 2 y 3 del artículo VIII del Código Procesal Penal son enfáticos al establecer que "*Carecen de efecto legal las pruebas obtenidas, directa o indirectamente, con violación del contenido esencial de los derechos*

fundamentales de la persona" y que "*La inobservancia de cualquier regla de garantía constitucional establecida a favor del procesado no podrá hacerse valer en su perjuicio*".

El procedimiento diseñado por el Ejecutivo generará **prueba prohibida**, es decir, medios de prueba que no podrán ser valorados por un Juez. Así, con la finalidad de agilizar la investigación e identificación del presunto autor, se han sacrificado derechos fundamentales. La consecuencia es irreversible: el proceso penal deberá excluir dichos medio de prueba[35] por lo que de nada habrá servido aquel procedimiento excepcional creado y administrado por el Ejecutivo.

Por lo señalado, el procedimiento de localización y geolocalización implementado por el Ejecutivo no es compatible con los Arts. IV, VI, IX, 202, 203 y 230 del del Código Procesal Penal. Tal y como Lawrence Lessig pronosticaba:

> (…) cuanto más se supervisa, más información investigable produce esta supervisión, la cual permanece disponible para ser investigada. Pero además del crecimiento de la información investigable, también está bajando los costes de la investigación. Y tal vez paradójicamente, esos costes decrecientes reduzcan las protecciones legales contra dicha investigación.[36]

El Poder Ejecutivo ha relajado nuestras garantías y derechos fundamentales para dotar de eficacia a la investigación policial. Sin embargo, atendiendo al principio de primacía de la Constitución, toda la información producida de este modo, no podrá ser empleada en el proceso penal, en respeto, precisamente, de aquellos derechos vulnerados.

5. CONCLUSIÓN

Se requiere una urgente modificación del Decreto Legislativo 1182 porque pone en riesgo la seguridad de todos los ciudadanos. Así, al encontrarnos en un Estado Constitucional de Derecho, exigimos que sea la autoridad judicial quien previamente autorice el acceso a información sensible como nuestros datos de geolocalización ya que se encuentran protegidos por los derechos del secreto de las comunicaciones, intimidad y autodeterminación informativa. Otorgarle esta facultad investigativa exclusivamente a una Unidad Especializada de la Policía, desplazando incluso a la Fiscalía, generará que los medios de prueba obtenidos no puedan ser utilizados en el proceso penal ya que constituyen prueba prohibida.

Apostar por relajar las garantías de los ciudadanos en aras de una supuesta eficacia investigativa no hará más que generar impunidad y reforzar aquella inseguridad ciudadana que el Decreto Legislativo pretende combatir. ■

NOTAS

1 Sobre la evolución de este fenómeno: MIRÓ LLINARES, Fernando. "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio". Buenos Aires: Marcial Pons, 2012. pp. 34-39. El citado autor destaca como ejemplos de ciberataques puros: hacking, malware intrusivo, malware destructivo, ataques de insiders, ataques DoS, ciberocupación red, antisocial networks. Ibid. p. 50.

2 "Con el surgimiento de nuevas tecnologías digitales y el advenimiento de Internet y la World Wide Web, la criminalidad organizada ha encontrado una herramienta sumamente útil para obtener mayor grado de eficacia en el desarrollo de actividades ilícitas. Históricamente el narcotráfico ha utilizado nuevas tecnologías para su funcionamiento de acuerdo con los últimos avances técnicos de época. Desde la utilización de teléfonos satelitales para las comunicaciones hasta la utilización de computadoras personales y agendas electrónicas de bolsillo para almacenar números de cuentas bancarias, direcciones de contacto personales, datos financieros, ventas y fórmulas para la fabricación de drogas. En la actualidad, tecnologías como tarjetas electrónicas, radios portátiles de banda ancha, teléfonos móviles clonados y la realización de reuniones por Internet de acceso reservado son algunas de las herramientas utilizadas alrededor del negocio del tráfico de drogas". SAIN, Raúl Gustavo. "Fraude, narcotráfico y lavado de dinero por internet". Buenos Aires: Editores del Puerto, 2012. p. 66

3 "A diferencia de otros tipos de delitos cometidos en la red, en la actualidad no existe estadística que permita establecer la magnitud de esa problemática a escala mundial. En diferentes países existe jurisprudencia en relación al blanqueo de fondos ilícitos mediante el uso de nuevas tecnologías. Al igual que en el mundo físico, los lavadores de dinero intentan eludir los sistemas tradicionales de prevención de manejo de dinero en efectivo y la vigilancia institucional del sistema bancario y financiero". Ibid. p. 85.

4 Entre las amenazas a la privacidad, destaca la *data gathering* (recolección de datos), *data exchanging* (intercambio de datos) y *data mining* (minería de datos). Ver: SCOLNIK, Hugo. "Qué es la seguridad informática". Buenos Aires: Paidós, 2014. pp. 166-167

5 PETRONE, Daniel. "Prueba informática". Buenos Aires: Ediciones Didot, 2014. p. 31.

6 Ibídem.

7 PÉREZ GIL, Julio. "Los datos sobre localización geográfica en la investigación penal". En: "Protección de datos y proceso penal". Madrid: La Ley, 2010. p. 310.

8 Si bien el artículo 2 del Decreto Legislativo prevé que la norma es aplicable a "teléfonos móviles o dispositivos electrónicos de naturaleza similar", en la página 2 de la Exposición de Motivos, el Ejecutivo dejó entrever sus alcances: "Las empresas que pre estos servicios son pieza clave en esta figura porque son el camino obligatorio que toman nuestras llamadas, **nuestros mensajes, correos electrónicos o nuestro acceso a Internet. Por esta razón, estas políticas se dirigen a ellos**". En el mismo sentido, El Comercio informó que: "El objetivo es localizar el teléfono **(también laptops, iPad y otros aparatos de comunicación)** desde donde provienen las llamadas extorsivas". EL COMERCIO. "En 2 meses la PNP geolocalizó 34 celulares de extorsionadores". Lima, 02 de febrero de 2016.

9 Entre los riesgos de la geolocalización se encuentran: "los seguimientos-trazabilidad de todo tipo de entidades (personas, animales, objetos), generación clandestina de perfiles-patrones (donde te encuentras, por donde te mueves, qué visitas, con quién te encuentras, cuánto tiempo estás, qué actividades haces, etc. vulnerando cuestiones relacionadas con la raza, política, religión, sexo, salud, etc.) para luego aplicarlos con herramientas de minería de datos (…) El geotagging permite conocer y señalar las coordenadas donde se encuentra una persona, casa (para robarla), se tomó una foto, bailamos, nos divertimos, hicimos negocios, restaurante, un lugar secreto, la localización de un evento, etc. pero como riesgo nos encontramos con la vigilancia social por GPS y la posibilidad que nos establezcan patrones de nuestros movimientos. Como contramedida sencilla frente al geotagging inhabilitar en el Smartphone o cámara de fotos (ya sea Android, iPhone o Blackberry) dicha característica que está activada por defecto". AREITIO, Javier. Análisis de aspectos de Ciberseguridad en Entornos de Geolocalización". En: Revista Española de Electrónica No. 696. Barcelona: Noviembre de 2012. p. 61.

10 GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS ESTABLECIDOS POR EL ARTÍCULO 29. "Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes". Adoptado el 16 de mayo de 2011. p. 4.

11 "Para lograr el fortalecimiento de la Policía Nacional del Perú es imprescindible brindar el marco legal necesario para la modernización de su capacidad operativa. En ese sentido, se requiere legislar sobre materias que posibiliten fortalecer la investigación criminal, la criminalística, el uso de tecnologías, establecer el beneficio de recompensas para promover y lograr la captura de miembros de organizaciones criminales, organizaciones terroristas y responsables de delitos de alta lesividad; mejorar la tipificación las Tablas de Infracciones y Sanciones del Régimen Disciplinario; así como la mejora en la estructura organizativa y la función policial, orientada a proveer servicios de calidad al ciudadano; medidas éstas que son necesarias para recuperar y fortalecer la confianza ciudadana en la Policía Nacional del Perú. Asimismo, es necesario regular el uso racional de la fuerza por parte de la Policía nacional como fuerza pública, conforme a estándares internacionales sobre la materia". Proyecto de Ley No. 4569-2014/PE "Ley que delega en el Poder Ejecutivo la facultad de legislar en materia de seguridad ciudadana, fortalecer la lucha contra la delincuencia y el crimen organizado". p. 06.

12 CONGRESO DE LA REPÚBLICA. Diario de los Debates. Sesión del 18 de junio de 2015. p. 193.

13 Ibíd. p. 215.

14 Ibíd. p. 225.

15 "Queremos aprovechar la figura jurídica de la flagrancia que nos da 24 horas, y la idea es la siguiente: poder solicitar inmediatamente la ubicación de ese teléfono para estar dentro de esas 24 horas y poder capturar a la persona". Ibíd. p. 240.

16 "Quisiera indicar, este proyecto no es para escuchar las conversaciones de los celulares, repito, no es para las escuchas, sino solamente para la ubicación del celular". Ibídem.

17 El profesor Mirco Musolesi, investigador de la Universidad de Birmingham, desarrolló un algoritmo con el que se podría predecir el crimen. Invito al lector a tomar consciencia sobre las implicancias que este modelo generará:
http://www.cambridgewireless.co.uk/Presentation/Location231013-University_Birmingham-Mirco_Musolesi.pdf
Por su parte, la División de Investigación y Desarrollo de Telefónica afirma que, entre los diferentes usos que se le puede dar a los datos móviles después de ser anonimizados, se encuentra la prevención de delitos: "(…) Utilizando el mismo tipo de datos de conducta, acumulados y **anónimizados** que se derivan de la actividad de la red móvil, obtenemos, en nuestra investigación experimental con datos reales sobre delitos en Londres, una precisión de casi un 70 % a la hora de predecir si una zona específica de la ciudad va a ser o no un foco de delitos". Recuperado de:
http://www.tid.es/es/innovacion-de-largo-plazo/prediccion-comportamiento-humano

18 Los únicos supuestos regulados en el Código Procesal Penal relacionados a las labores de prevención del delito están establecidos en los Arts. 205 y 213, los cuales están referidos al control de identidad policial y al examen corporal para las pruebas de alcoholemia, respectivamente.

19 "En tal sentido, el hecho de intervenir comunicaciones para usar datos derivados de éstos para la identificación, localización o geolocalización de otros equipos de comunicación, en sí representa una intervención en las comunicaciones de los titulares de los equipos, y dicha conducta se encuentra prohibida por abarcar el derecho constitucional al secreto e inviolabilidad de las comunicaciones y documentos privados previsto en el numeral 10 del artículo 2 de la Constitución (…)". CARO CORIA, Carlos. "La inconstitucionalidad de la ley de localización y geolocalización". Lima: La Ley, 31 de julio de 2015. Recuperado de:
http://laley.pe/not/2643/la-inconstitucionalidad-de-la-ley-de-lsquo-localizacion-rsquo-y-lsquo-geolocalizacion-rsquo-/

20 STC recaída en el Expediente No. 00655-2010-PHC/TC del 27 de octubre de 2010. Segundo pár. del Fund. 18.

21 "(…) El artículo 11 se aplican a las conversaciones telefónicas independientemente de su contenido, 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, la hora, duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones". Fundamento 114.

22 "No obte y pese a esta postura inicial, tanto la jurisprudencia del TEDH como la de nuestro Tribunal Constitucional –con refrendo posterior del legislador comunitario (Directiva 2005/54/CE) y del legislador nacional (Ley 25/2007)-, han dejado claro que **los datos de tráfico forman parte del derecho al secreto de las comunicaciones**, y que es la ley que regula el acceso a las mismas la que debe prever los presupuestos, requisitos, procedimientos y tratamiento de los datos periféricos de la correspondiente comunicación. FLORES PRADA, Ignacio. "Criminalidad informática. Aspectos sutivos y procesales". Valencia: Tirant lo Blanch 2012. p. 357.

23 "El derecho a la intimidad o a la vida privada involucra al conjunto de actos, situaciones o circuncias que, por su carácter personalísimo, no se encuentran normalmente expuestos al dominio público. Protege tanto la intimidad de la persona como la de su familia, y comprende la libertad del individuo de conducirse en determinados espacios y tiempo, libre de perturbaciones ocasionadas por terceros, así como la facultad de defenderse de la divulgación de hechos priva. El derecho a la intimidad se proyecta en dos dimensiones como secreto de la vida privada y como libertad. **Concebida la intimidad como secreto**, atentan contra ella todas las intromisiones o divulgaciones ilegítimas respecto a hechos relacionados con la vida privada o familiar, o las investigaciones también ilegítimas de acontecimientos propios de dicha vida. **Concebida como libertad individual**, la intimidad trasciende y se realiza en el derecho de toda persona a tomar por sí sola decisiones que conciernen a la esfera de su vida privada. La vulneración de la intimidad personal y familiar se produce por la sola intromisión externa o perturbación no autorizadas en las áreas privadas o reservadas (actos, hechos, hábitos, datos) que comprende, así como con las divulgaciones de su contenido sin contar con el consentimiento de su titular)". RUBIO CORREA, Marcial y otros. "Los derechos fundamentales en la jurisprudencia del Tribunal Constitucional. Análisis de los artículos 1, 2 y 3 de la Constitución". Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú, 2013. pp. 347 y s. En el mismo sentido, el Tribunal Constitucional sostiene que: "(…) la vida privada se encuentra constituida por "los datos, hechos o situaciones desconocidas 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" [STC 0009-2007-PI/TC y otros, fundamento 43] De esta forma, la intimidad se presenta como una libertad en sentido negativo, en tanto excluye o impide que terceros –entre ellos, claro está, el mismo Estado- puedan acceder a determinados contenidos que la propia persona desea resguardar. (…) En el caso concreto de la intimidad, se demanda lo que en su momento la doctrina anglosajona denominó *right to be alone*, esto es, el derecho a no ser perturbado. La consecuencia natural del ejercicio de este ámbito del derecho a la intimidad es, que la persona tenga la posibilidad de […] tomar decisiones relacionadas con diversas áreas de de la propia vida libremente, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público [Corte Interamericana de Derechos Humanos en el Caso Fontevecchia y D´Amico vs. Argentina. Sentencia de Fondo de 29 de noviembre de 2011, párr. 48]". STC Exp. 00009-2014-PI/TC emitida el 04 de marzo de 2016. Fundamentos 4, 6 y 7.

24 "El concepto de intimidad tradicional debe ampliarse a fin de incorporar una nueva tutela del ciudadano, que podría llamarse tutela al derecho de autodeterminarse en una sociedad informativa (…) En lo personal, considero que podría discutirse si se trata de una efectiva ampliación del concepto tradicional o que el antes mencionado opera como un complemento de aquél, pero a todo evento, es clara la imposibilidad de quedarse atado a una concepción cristalizada en un momento anterior a la *sociedad informatizada*". RIQUERT, Marcelo Alfredo. "Protección penal de la intimidad en el espacio virtual". Buenos Aires: Ediar, 2003. p. 51.

25 CARO CORIA, Carlos. Op. Cit.

26 Hasta hace algunos años, el Tribunal Constitucional reconocía que bastaba con la concurrencia de uno de los supuestos; es decir, la inmediatez temporal o personal. Sobre el particular, ver: STC Exp. 3766-2004-PH/TC. Caso Menor IV, Ch; STC Exp. 5451-2005-PHC/TC. Caso Carlos Rodríguez Olano; STC Exp. 1923-2006-PHC/TC. Caso Jorge Manuel Chipulina Fernández; STC Exp. 05696-2009-PHC/TC. Caso Henrry Heli Bustamante Campos.

27 STC Exp. 04630-2013-PHC/TC. Caso José Fermín Maqui Salinas. Fundamento No. 3.3.3. Reciente jurisprudencia constitucional ha seguido la misma línea argumentativa: STC Exp. 00354-2011-PHC/TC. Caso Noé Huamán Ayma y otros; STC Exp. 03731-2012-PHC/TC. Caso Orlando Gavidia Vega y otros.

28 "El pasado 1 de diciembre, un hombre denunció en la comisaría del Callao el secuestro de su esposa, Juana Pinedo Pacaya, de 24 años. Dijo que los supuestos delincuentes lo llamaban desde un celular y le pedían S/. 5 mil para no matarla. El número de ese teléfono fue clave para conocer la verdad. El caso fue derivado al nuevo Departamento de Geolocalización de la Policía, situado en la Dirección de investigación Criminal (Dirincri) de la avenida España. Los agentes solicitaron la ubicación de este celular a la empresa operadora. En solo una hora ya se sabía que el secuestrador se comunicaba desde Comas. De inmediato, la Policía fue al lugar y encontró a Juana Pinedo paseando con otro sujeto por Lima norte. Fue un autosecuestro". EL COMERCIO. "En 2 meses la PNP geolocalizó 34 celulares de extorsionadores". Lima: 08 de febrero de 2016.

29 De acuerdo al artículo 8 del Decreto Legislativo, los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios están exentos de responsabilidad por el suministro de datos de localización o geolocalización, en el marco del presente decreto legislativo.

30 Curiosamente, la prensa difundió la idea que el Decreto Legislativo se restringía únicamente a casos de extorsión. Así, por ejemplo, el 30 de agosto de 2015, el Diario La República publicó el siguiente titular: "80% de peruanos está de acuerdo con la ley de geolocalización". En el artículo se sentencia que: "Al responder sobre si aprobaban <el decreto que permite a la Policía acceder a la ubicación geográfica (geolocalización) de los celulares desde los cuales se realicen extorsiones, como medida para ponerle fin al sicariato>, un abrumadora mayoría (80% de los encuestados) respondió que sí estaba de acuerdo". Como se puede apreciar, la pregunta efectuada por la encuestadora estaría mal formulada ya que se centra en uno o dos delitos de gravedad pero, al parecer, no habría informado sobre todo el catálogo de delitos que permiten la geolocalización de los dispositivos. Recuperado de: http://larepublica.pe/sociedad/699664-80-de-peruanos-e-de-acuerdo-con-la-ley-de-geolocalizacion

31 Al firmar el Protocolo de Geolocalización, el 16 de octubre de 2015, el Ministro Pérez Guadalupe afirmó: "Frente a una denuncia en cualquier comisaría, ésta pasará a la unidad especializada, quien a su vez comunica al fiscal, quien de manera inmediata verifica el delito flagrante, que la sanción del delito sea mayor de 4 años y que la geolocalización sea necesaria para la investigación". AGENDA PAÍS. "Mininter: Policía Nacional y empresas de telefonía firmaron protocolo de geolocalización". Recuperado de: www.agendapais.com/?p=28056

32 artículo 331 CPP.- 1. Tan pronto la Policía tenga noticia de la comisión de un delito, lo pondrá en conocimiento del Ministerio Público por la vía más rápida y también por escrito, indicando los elementos esenciales del hecho y demás elementos inicialmente recogidos, así como la actividad cumplida, sin perjuicio de dar cuenta de toda la documentación que pudiera existir.

33 El profesor español Francisco Muñoz Conde critica la flexibilización en el tratamiento de las prohibiciones probatorias (entre ellas, las escuchas telefónicas) manifedo que con ello se están vulnerando derechos fundamentales: "Como seguidamente vamos a ver, se pronuncian hoy en día cada vez más decisiones jurisprudenciales que de un modo u otro evaden las dificultades probatorias que se derivan del *nemo tenetur* y se elaboran teorías que cuestionan o debilitan en parte las estrictas prohibiciones probatorias, incluso las derivadas de la práctica de la tortura, en determinados casos y supuestos (principalmente terrorismo y delincuencia organizada), que se alegan para justificar la creación de lo que el profesor Günther Jakobs ha llamado con expresión que ha hecho fortuna Derecho penal del enemigo y que aquí con más propiedad podríamos llamar Derecho procesal penal del enemigo". MUÑOZ CONDE, Franciso. "De las prohibiciones probatorias al Derecho procesal penal del enemigo". Buenos Aires: Hamurabi, 2008. p. 29. El Gobierno justificó la promulgación del Decreto Legislativo 1182 en la necesidad de combatir de manera rápida y eficiente delitos graves como la extorsión; sin embargo, en esta lucha, no dudó en sacrificar nuestros derechos. De allí que transpolemos las críticas del Derecho Penal del Enemigo ya que éste, "tal y como lo ha formulado Jakobs es incompatible con el vigente Estado democrático de derecho español. Resulta no solo peligrosa, sino totalmente errónea la idea de que los derechos fundamentales y ciertas garantías propias de dicho sistema son solo para quien se las gana". FEIJÓO SÁNCHEZ, Bernando. "El derecho penal del enemigo y el Estado democrático de derecho". En: Derecho Penal Contemporáneo. Revista Internacional No. 16. Bogotá: Legis, 2006. p. 176

[34] En el mismo sentido: "la ley procesal establece dentro de los alcances de la medida de levantamiento de secreto de comunicaciones dictada por el juez, la obligación de las empresas concesionarias de brindar la geolocalización de teléfonos móviles, e inclusive dicha norma es más clara porque establece que dicha medida podrá dictarse no sólo contra el investigado sino también 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. De esta forma, quedan en evidencia las ambigüedades, vacíos y contradicciones que trae consigo el Decreto Legislativo N° 1182, cuyo problema central radica en haberse otorgado facultades a la Policía para solicitar la intervención de comunicaciones para la identificación, localización y geolocalización de equipos, sin orden ni control judicial alguno". CARO CORIA, Carlos. Op. Cit.

[35] La prueba ilícita, en el sentido aquí expuesto, esto es, en cuanto obtenida con vulneración de derechos constitucionales, tendrá como efecto su *inutilizabilidad*, lo cual conlleva, a su vez, la prohibición de su admisión así como de su valoración en el proceso. Lo dicho implica que deba declararse este efecto y proceder a la exclusión del material probatorio ilícito inmediatamente que se conozca, puesto que no se trata simplemente de una prohibición de valoración, pues esto último implicaría que solo sea analizada en el juicio oral, resultando que la ilicitud derivada de la vulneración de derechos fundamentales produciría efectos menos intensos que una nulidad procesal, cuya declaración puede operarse de oficio en cuanto es conocida. ASCENCIO MELLADO, José María, citado por: VILLEGAS PAIVA, Elky Alexander. "La regla de exclusión de la prueba ilícita: Fundamento, efectos y excepciones". Lima: Instituto Pacífico, 2015. p. 225 y s.

[36] Citado por PETRONE, Daniel. "Prueba informática". Buenos Aires: Ediciones Didot, 2014. p. 20.