Análisis sobre la inconstitucionalidad del Decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Federal de Procedimientos Penales, del Código Penal Federal, de la Ley Federal de Telecomunicaciones, de la Ley que establece las Normas Mínimas sobre Readaptación Social de Sentenciados y de la Ley General del Sistema Nacional de Seguridad Pública, publicadas en el Diario Oficial de la Federación el día 17 de abril de 2012.[1]

Introducción

El día 17 de Abril de 2012 fue publicado en el Diario Oficial de la Federación el Decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Federal de Procedimientos Penales, del Código Penal Federal, de la Ley Federal de Telecomunicaciones, de la Ley que establece las Normas Mínimas sobre Readaptación Social de Sentenciados y de la Ley General del Sistema Nacional de Seguridad Pública (en adelante "el Decreto").[2]

Del proceso legislativo se desprende que las reformas, adiciones y derogaciones que contiene el Decreto tienen por objeto, de manera general, el fortalecer las capacidades de las autoridades investigadoras para combatir de manera más eficaz delitos de innegable gravedad como lo son el secuestro y la extorsión. Cabe señalar que el Decreto viene a sustituir diversas disposiciones que, de igual manera que el Decreto objeto de análisis, tenían la intención de otorgar mejores herramientas a

[1] Análisis elaborado por Luis Fernando García Muñoz. Licenciado en Derecho por la Universidad Iberoamericana. Candidato a Maestro en Derecho Internacional de los Derechos Humanos y Derecho de Propiedad Intelectual por la Universidad de Lund, Suecia.

[2] Decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Federal de Procedimientos Penales, del Código Penal Federal, de la Ley Federal de Telecomunicaciones, de la Ley que establece las Normas Mínimas sobre Readaptación Social de Sentenciados y de la Ley General del Sistema Nacional de Seguridad Pública publicado en el Diario Oficial de la Federación el 17 de abril de 2012.

las autoridades para combatir a la delincuencia, pero que por su inadecuada regulación, los graves riesgos que implicaron (y siguen implicando) para los derechos humanos e incluso por no resultar factibles desde un punto de vista técnico fracasaron.

En concreto, de las reformas llevadas a cabo en el año 2009[3], destaca la creación del Registro Nacional de Usuarios de Telefonía Móvil (*RENAUT*), el cual, debido a su inadecuada regulación, presentaba serios riesgos a la privacidad y seguridad de los usuarios. Si bien resulta un avance la cancelación de este registro, el mecanismo diseñado por el Decreto para sustituir al *RENAUT*, consistente en el otorgamiento de facultades a autoridades investigadoras y el establecimiento de obligaciones para los concesionarios y permisionarios de servicios de telecomunicaciones para permitir la localización geográfica, en tiempo real, de cualquier equipo de comunicación móvil, presenta serias deficiencias que significan una vulneración a los derechos humanos de los usuarios de servicios de telefonía móvil.

El presente análisis se concentrará en la inconstitucionalidad las disposiciones relacionadas con el sistema de localización geográfica en tiempo real de equipos de comunicación móvil. Por el contrario, este análisis no comprende aquellas disposiciones contenidas en el Decreto que facultan otro tipo de medidas, por ejemplo, en relación con el bloqueo de señales en establecimientos penitenciarios.

El objeto de este análisis es el de coadyuvar con la Comisión Nacional de los Derechos Humanos para que en cumplimiento de su obligación constitucional de protección de los derechos humanos ejerza la facultad que establece el artículo 105 fracción II inciso g) de la Constitución Política de los Estados Unidos Mexicanos (en adelante "la Constitución") y presente una acción de inconstitucionalidad respecto de diversas disposiciones contenidas en el Decreto.

[3] Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones publicado en el Diario Oficial de la Federación el 9 de febrero de 2009.

Para ello, en primer lugar se hará mención de las obligaciones generales del Estado Mexicano respecto de los derechos humanos contenidas en el artículo primero de la Constitución, los artículos 1.1 y 2 de la Convención Americana sobre Derechos Humanos (en adelante "CADH" o "la Convención") y el artículo 2 del Pacto Internacional de Derechos Civiles y Políticos (en adelante "PIDCP" o "el Pacto").

Posteriormente, se hará un análisis sobre el contenido y alcance del derecho a no ser objeto de injerencias arbitrarias o ilegales en la vida privada, familiar, el domicilio, la correspondencia o las comunicaciones privadas (en adelante genéricamente denominado "Derecho a la Privacidad" salvo mención expresa de alguno de sus componentes) contenida en el artículo 16º de la Constitución, el artículo 11 de la CADH y el artículo 17 del PIDCP.

Finalmente, se realizará el análisis de las diversas disposiciones del Decreto que contravienen los derechos humanos contenidos en la Constitución y los tratados internacionales en materia de derechos humanos. En concreto, el artículo 133 Quáter del Código Federal de Procedimientos Penales, los artículos 3 fracción XVII, 40 Bis, 44 fracciones XVI y XVII, 71 apartado A fracción VI y artículos Transitorios Tercero y Cuarto de la Ley Federal de Telecomunicaciones y el artículo 178 Bis del Código Penal Federal.

La observancia de las obligaciones generales en materia de derechos humanos en la adopción de medidas legislativas.

Resulta pertinente recordar que a partir de la reforma constitucional en materia de derechos humanos publicada en el Diario Oficial de la Federación el día 10 de junio de 2011, en el artículo 1º fueron consagrados los principios y obligaciones rectores de la actividad del Estado respecto de los derechos humanos establecidos en la Constitución y en los tratados internacionales.

Cabe destacar que a partir de la reforma constitucional, todas las autoridades del Estado Mexicano se encuentran obligadas a promover, respetar, proteger y garantizar los derechos humanos. Asimismo, a partir de dicha reforma fue

reconocido el principio de interpretación conforme de los derechos humanos con la Constitución y los tratados internacionales a la luz del principio *pro persona.*

En atención a ello, resulta de particular importancia mencionar que los artículos 2 de la CADH[4] y del PIDCP[5] ponen en cabeza del Estado Mexicano, la obligación de adoptar las disposiciones legislativas o de cualquier otro carácter que sean necesarias para hacer efectivos los derechos humanos reconocidos en dichos tratados.

En interpretación de dicha obligación, la Corte Interamericana de Derechos Humanos (en adelante "*Corte IDH*") ha resaltado lo siguiente:

> *"[L]a adecuación de la normativa interna a los parámetros establecidos en la Convención implica la adopción de medidas en dos vertientes, a saber: a) la supresión de las normas y prácticas de cualquier naturaleza que entrañen violación a las garantías previstas en la Convención o que desconozcan los derechos allí reconocidos u obstaculicen su ejercicio, y b) la expedición de normas y el desarrollo de prácticas conducentes a la efectiva observancia de dichas garantías. La primera vertiente se satisface con la reforma, la derogación, o la anulación de las normas o prácticas que tengan esos alcances, según corresponda. La segunda, obliga al Estado a prevenir la recurrencia de violaciones a los derechos humanos y, por eso, debe adoptar todas las medidas legales, administrativas y de otra índole que sean necesarias […]".*[6]

---

[4] Artículo 2. Deber de Adoptar Disposiciones de Derecho Interno.
Si en el ejercicio de los derechos y libertades mencionados en el artículo 1 no estuviere ya garantizado por disposiciones legislativas o de otro carácter, los Estados partes se comprometen a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones de esta Convención, las medidas legislativas o de otro carácter que fueren necesarias para hacer efectivos tales derechos y libertades.

[5] Artículo 2.2
Cada Estado Parte se compromete a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones del presente Pacto, las medidas oportunas para dictar las disposiciones legislativas o de otro carácter que fueren necesarias para hacer efectivos los derechos reconocidos en el presente Pacto y que no estuviesen ya garantizados por disposiciones legislativas o de otro carácter.

[6] Corte IDH. *Caso Castillo Petruzzi y otros Vs. Perú*. Fondo, Reparaciones y Costas. Sentencia de 30 de mayo de 1999 Serie C No. 52, párr. 207; *Caso Salvador Chiriboga Vs. Ecuador*. Excepción Preliminar y Fondo. Sentencia de 6 de mayo de 2008 Serie C No. 179, párr. 122; y Caso *Fontevecchia y D' Amico*

En este sentido, la Corte IDH ha señalado que la promulgación de una ley contraria a las obligaciones asumidas por un Estado parte de la CADH constituye una violación de lo dispuesto por el artículo 2 de la Convención.[7]

De esta forma, a la luz de las obligaciones generales y los principios establecidos en el artículo 1º de la Constitución, así como en los artículos 1.1 y 2 de la CADH y 2 del PIDCP, es claro que la adopción de disposiciones contrarias a las obligaciones emanadas de cualquier derecho humano resultan en sí mismas una violación de ese derecho y por tanto dichas disposiciones resultan violatorias de la Constitución.

Las disposiciones del Decreto en materia de Geolocalización.

Las principales disposiciones del Decreto que levantan serios cuestionamientos sobre su constitucionalidad son la adición del artículo 133 Quáter al Código Federal de Procedimientos Penales, la adición de un artículo 40 Bis, y de las fracciones XVI y XVII al artículo 44 de la Ley Federal de Telecomunicaciones. A continuación se transcriben:

Código Federal de Procedimientos Penales.

> *"Artículo 133 Quáter. Tratándose de investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas, el Procurador General de la República o los servidores públicos en quienes delegue la facultad, solicitarán por simple oficio o medios electrónicos a los concesionarios o permisionarios del servicio de telecomunicaciones la localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea, que se encuentren*

Vs. Argentina. Fondo, Reparaciones y Costas. Sentencia de 29 de noviembre de 2011. Serie C No. 238, párr. 85.

[7] Corte IDH. *Ciertas Atribuciones de la Comisión Interamericana de Derechos Humanos.* Opinión Consultiva OC-14/94 del 9 de diciembre de 1994. Serie A No. 13, párr. 26; y *Responsabilidad Internacional por Expedición y Aplicación de Leyes Violatorias de la Convención*. Opinión Consultiva OC-14/94 del 9 de diciembre de 1994. Seria A No. 14, párr. 50.

relacionados.

De todas las solicitudes, la autoridad dejará constancia en autos y las mantendrá en sigilo.

En ningún caso podrá desentenderse la solicitud y toda omisión imputable al concesionario o permisionarios, será sancionada en términos de lo previsto por el artículo 178 Bis del Código Penal Federal.

Se castigará a la autoridad investigadora que utilice los datos e información obtenidos como resultado de localización geográfica de equipos de comunicación móvil para fines distintos a los señalados en este artículo, en términos de lo establecido en la fracción IV del artículo 214 del Código Penal Federal."

Ley Federal de Telecomunicaciones

"Artículo 40 BIS. Los concesionarios o permisionarios del servicio de telecomunicaciones, están obligados a colaborar con las autoridades en la localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea que se encuentren relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas a solicitud del Procurador General de la República, de los procuradores de las entidades federativas o de los servidores públicos en quienes deleguen esta facultad, de conformidad con las leyes correspondientes.

Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por el artículo 178 BIS del Código Penal Federal.

Artículo 44. Los concesionarios de redes públicas de telecomunicaciones deberán:

XVI. Contar con sistemas, equipos y tecnologías que permitan la ubicación o localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea.

XVII. Asignar un área con responsables operativos en la función de colaborar con las autoridades en la localización geográfica, en tiempo real, de los equipos de comunicación móvil que se encuentren relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas."

De las disposiciones transcritas se desprende el otorgamiento de la facultad a la Procuraduría General de la República (PGR) de obtener, por medio de un simple oficio o medio electrónico dirigido a los concesionarios o permisionarios de servicios de telecomunicaciones, los datos de localización geográfica, en tiempo real, de cualquier equipo de comunicación móvil que se encuentre relacionado con alguna investigación respecto de ciertos delitos. Es importante resaltar que la facultad otorgada no requiere la obtención de autorización previa por parte de la autoridad judicial federal y si bien las solicitudes deben constar en autos, por la propia naturaleza de la facultad, éstas deben mantenerse en sigilo, es decir, fuera del conocimiento de cualquier persona. A su vez se imponen a los concesionarios y permisionarios de servicios de telecomunicaciones obligaciones consistentes en la imposibilidad de incumplir con las solicitudes de la PGR y las procuradurías de las entidades federativas, además de diversas obligaciones de carácter operativo para hacer posible la implementación de la facultad.

Asimismo, las disposiciones contenidas en los artículos 178 Bis del Código Penal Federal y los artículos 3 fracción XVII, 71, apartado A, fracción VI y los artículos Transitorios Tercero y Cuarto del Decreto que reforma, adiciona y deroga la Ley Federal de Telecomunicaciones, también verían afectada su constitucionalidad en caso de que la facultad descrita en las disposiciones principales sea declarada inconstitucional.

Para determinar si la obtención de datos de geolocalización en los términos que establece el Decreto se ajusta a los requerimientos constitucionales y convencionales en materia de derechos humanos es necesario analizar el contenido y alcance de las disposiciones relevantes a la luz de su interpretación por los órganos autorizados, así como a la luz del derecho comparado, no perdiéndose de vista en ningún momento el principio de interpretación *pro persona* y las obligaciones generales del Estado Mexicano en materia de derechos humanos, especialmente las atinentes al deber de adoptar disposiciones de derecho interno de manera compatible con dichas obligaciones.

Las Disposiciones del Decreto en Materia de Geolocalización a la luz del Derecho a la Privacidad y la Inviolabilidad de las Comunicaciones Privadas

El artículo 11 de la CADH[8] y el artículo 17 del PIDCP[9] reconocen el derecho de toda persona a no ser objeto de injerencias arbitrarias o abusivas en su vida privada, la de su familia, en su domicilio o en su correspondencia, así como el derecho a la protección de la ley contra esas injerencias o ataques.

En reiteradas ocasiones[10] el Poder Judicial de la Federación (PJF) ha entendido que el derecho a la vida privada, a la privacidad o a la intimidad, como ha sido distintamente denominado, se encuentra también protegido por el párrafo primero del artículo 16 de la Constitución y en algunas vertientes específicas también protegido por otras disposiciones constitucionales como lo es la

[8] Artículo 11
1. (…)
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, no 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.

[9] 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.

[10] Véase por ejemplo, Tesis: 2ª. LXIII/2008, Novena Época, 2ª Sala, Semanario Judicial de la Federación y su Gaceta, Tomo XXVII, Mayo de 2008, página 229. Rubro: DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

protección de datos personales a que se refiere el artículo 7 y el párrafo segundo del artículo 16.

Como la Corte IDH ha señalado, lo que el derecho a la privacidad protege esencialmente es "el ámbito de la privacidad [el cual] se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública"[11].

De manera relacionada con el derecho a la privacidad o intimidad en general, se encuentra la protección a la inviolabilidad de las comunicaciones privadas, la cual posee una protección constitucional específica en los párrafos decimosegundo y decimotercero del artículo 16 como a continuación se transcribe:

> *"Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.*
>
> *Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor."*

[11] Corte IDH. Caso *Tristán Donoso Vs. Panamá*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 27 de enero de 2009 Serie C No. 193, párr. 55; *Caso Escher y otros Vs. Brasil*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 113; y *Caso Fernández Ortega y otros Vs. México*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 30 de agosto de 2010. Serie C No. 215, párr. 157.

Al respecto, la Suprema Corte de Justicia de la Nación (SCJN) ha interpretado que las comunicaciones privadas objeto de protección no se circunscriben solamente a la correspondencia de carácter escrito, sino que también comprende las comunicaciones realizadas por cualquier medio o artificio técnico desarrollado a la luz de las nuevas tecnologías:

Novena Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXXIV, Agosto de 2011
Página: 217
Tesis: 1a. CLVIII/2011
Tesis Aislada
Materia(s): Constitucional

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. MEDIOS A TRAVÉS DE LOS CUALES SE REALIZA LA COMUNICACIÓN OBJETO DE PROTECCIÓN.

Tradicionalmente, las comunicaciones privadas protegidas en sede constitucional han sido identificadas con la correspondencia de carácter escrito, que es la forma más antigua de comunicarse a distancia entre las personas. De ahí que en el penúltimo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, se señale que "la correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro". Sin embargo, la expresa referencia a las comunicaciones postales no debe interpretarse como una relación cerrada. En primer término, es necesario señalar ***que nuestra Constitución no limita los medios a través de los cuales se puede producir la comunicación objeto de protección del derecho fundamental*** *en estudio. Esto resulta acorde con la finalidad de la norma, que no es otra que la libertad de las comunicaciones, siendo que* ***ésta puede ser conculcada por cualquier medio o artificio técnico desarrollado a la luz de las nuevas***

tecnologías. Del tradicional correo o telégrafo, pasando por el teléfono alámbrico y el teléfono móvil, hemos llegado a las comunicaciones que se producen mediante sistemas de correo electrónico, mensajería sincrónica o instantánea asincrónica, intercambio de archivos en línea y redes sociales. *Las posibilidades de intercambio de datos, informaciones y mensajes se han multiplicado por tantos programas y sistemas como la tecnología es capaz de ofrecer y, por lo tanto, también las maneras en que dichos contenidos pueden ser interceptados y conocidos por aquellos a quienes no se ha autorizado expresamente para ello. En definitiva****, todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, deben quedar protegidas por el derecho fundamental a la inviolabilidad de las comunicaciones privadas. (énfasis añadido)***

Amparo directo en revisión 1621/2010. 15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

De esta forma la SCJN ha precisado que lo que el derecho a la inviolabilidad de las comunicaciones prohíbe, es la "intercepción o el conocimiento antijurídico de una comunicación ajena".[12] A su vez ha señalado que este derecho "se configura como una garantía formal, esto es, las comunicaciones resultan protegidas con independencia de su contenido. En este sentido, no se necesita en modo alguno analizar el contenido de la comunicación o de sus circunstancias, para determinar su protección por el derecho fundamental."[13] Por lo tanto "la violación de este derecho se consuma en el momento en que se escucha, se graba, se almacena, se lee o se registra -sin el consentimiento de los interlocutores-, una comunicación ajena"[14].

Resulta determinante para el presente análisis el observar que la SCJN, al

[12] Tesis: 2ª. LXIII/2008, Novena Época, 1ª Sala, Semanario Judicial de la Federación y su Gaceta, Tomo XXXIV, Agosto de 2011, página 221. Rubro: DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SUS DIFERENCIAS CON EL DERECHO A LA INTIMIDAD. Amparo directo en revisión 1621/2010. 15 de junio de 2011.
[13] Id.
[14] Id.

interpretar el derecho a la inviolabilidad de las comunicaciones privadas ha determinado que su objeto comprende no sólo el contenido de las comunicaciones, sino también los datos externos que identifican la comunicación:

Novena Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXXIV, Agosto de 2011
Página: 221
Tesis: 1a. CLV/2011
Tesis Aislada
Materia(s): Constitucional

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE IDENTIFICAN LA COMUNICACIÓN.

El objeto de protección constitucional del derecho a la inviolabilidad de las comunicaciones privadas, previsto en el artículo 16, párrafos decimosegundo y decimotercero, de la Constitución Política de los Estados Unidos Mexicanos, no hace referencia únicamente al proceso de comunicación, sino también a aquellos datos que identifican la comunicación. A fin de garantizar la reserva que se predica de todo proceso comunicativo privado, resulta indispensable que los datos externos de la comunicación también sean protegidos. Esto se debe a que, si bien es cierto que los datos no se refieren al contenido de la comunicación, también lo es que en muchas ocasiones ofrecen información sobre las circunstancias en que se ha producido la comunicación, afectando así, de modo directo o indirecto, la privacidad de los comunicantes. Estos datos, que han sido denominados habitualmente como "datos de tráfico de las comunicaciones", deberán ser objeto de análisis por parte del intérprete, a fin de determinar si su intercepción y conocimiento antijurídico resultan contrarios al derecho fundamental en cada caso concreto. Así, de modo ejemplificativo, el registro de los números marcados por un usuario de la

red telefónica, la identidad de los comunicantes, la duración de la llamada telefónica o la identificación de una dirección de protocolo de internet (IP), llevados a cabo sin las garantías necesarias para la restricción del derecho fundamental al secreto de las comunicaciones, puede provocar su vulneración.

Amparo directo en revisión 1621/2010. 15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

Lo anterior también ha sido reconocido por la Corte IDH, que en el caso *Escher vs. Brasil*, relativo a intervenciones telefónicas, señaló lo siguiente:

"El artículo 11 se aplica 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. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación."[15]

De esta forma, de acuerdo con los precedentes citados y en atención al principio de interpretación *pro persona* consagrado en el artículo 1º Constitucional y el artículo 29 de la CADH, es claro que los "datos de tráfico" de comunicaciones se encuentran igualmente protegidos por la garantía formal contenida en los párrafos decimosegundo y decimotercero del artículo 16 de la Constitución.

---

[15] Corte IDH. *Escher Vs, Brasil*, supra nota 11, párr. 114. Ver también de la Corte Europea de Derechos Humanos (ECHR). *Case of Malone v. United Kingdom*. Judgment of 2 August 1984, application no. 8691/79.

Por su parte, los datos de localización geográfica son datos que sin duda se encuentran dentro del ámbito de protección del artículo 16 Constitucional, 11 de la CADH y 17 del PIDCP. Cuando esos datos son obtenidos a través de equipos de comunicación o el monitoreo o registro de comunicaciones es claro que deben ser considerados como "datos de tráfico" de comunicaciones protegidos por el derecho a la inviolabilidad de las comunicaciones privadas.

Algunos precedentes que pueden encontrarse en la jurisprudencia internacional comparada soportan lo sostenido anteriormente. Por ejemplo, la Corte Europea de Derechos Humanos (ECHR) estableció en el caso *Uzun v. Germany*[16] que métodos de vigilancia que implican el monitoreo, registro o uso de información obtenida a través de un dispositivo GPS (Sistema de Posicionamiento Global) alojado en un automóvil constituye una interferencia en la vida privada de acuerdo al artículo 8 de la Convención Europea de Derechos Humanos, que establece el derecho a la privacidad de manera similar a la CADH y el PIDCP.

De igual manera, recientemente la Suprema Corte de los Estados Unidos de América decidió en el caso *United States v. Jones*[17] que la colocación de un dispositivo GPS en el auto de *Jones* violaba la 4ta enmienda de la Constitución de los Estados Unidos, disposición que establece protecciones similares a las contenidas en el artículo 16 de la Constitución. Aunque algunos de los jueces se basaron principalmente en la transgresión a la propiedad del inculpado para la colocación del dispositivo para declarar la violación, la Jueza Sotomayor detalla en su voto concurrente que la obtención de información a través de métodos tecnológicos no invasivos (*non-trespassory surveillance techniques*), como la vigilancia a través de dispositivos de geolocalización, implican una afectación a las expectativas razonables de privacidad[18].

El concepto de "expectativa razonable de privacidad" para determinar el alcance de la protección del derecho a la privacidad, puede resultar relevante para el

[16] ECHR. *Case of Uzun v. Germany*. Judgment of 2 September 2010, application no. 35623/05.
[17] *U.S. v Jones* 10 U.S. 1259 (2011)
[18] Ibidem, J. Sotomayor concurring.

presente análisis. Dicho concepto desarrollado por la Suprema Corte de los Estados Unidos en el caso *Katz v. United States*[19], ha sido recogido ampliamente por la jurisprudencia de la Corte Europea de Derechos Humanos[20] y también recientemente de manera tangencial por la Corte IDH[21].

En este sentido, como detalla la Jueza Sotomayor, la vigilancia a través de mecanismos de geolocalización genera información precisa y amplia sobre los movimientos públicos de una persona, lo cual refleja una gran cantidad de detalles sobre sus asociaciones políticas, profesionales, familiares, religiosas y sexuales[22], por lo tanto es claro que las personas poseen una expectativa razonable de privacidad sobre sus datos de localización geográfica y por ende estos datos se encuentran protegidos por el derecho a la privacidad establecido en el artículo 16 constitucional, 11 de la CADH y 17 del PIDCP.

Los datos de localización vinculados con equipos de comunicación además deben ser tratados como "datos de tráfico" de comunicaciones a los cuáles les resulta aplicable la garantía formal establecida en los párrafos decimosegundo y decimotercero del artículo 16 constitucional. Lo anterior queda corroborado en tanto el artículo 44 fracción XII incisos d) y e) de la Ley Federal de Telecomunicaciones consideran como datos que deben conservarse dentro de un registro de comunicaciones, a los datos referentes a la localización de activación del servicio y la ubicación digital del posicionamiento geográfico de las líneas telefónicas.[23] Si los datos históricos de localización geográfica de comunicaciones y líneas telefónicas resultan "datos de tráfico" de comunicaciones, con mayor razón el monitoreo prospectivo en tiempo real de dichos datos debe gozar de la misma protección constitucional, sino es que mayores salvaguardas resultan necesarias.

---

[19] *Katz v. United States*, 389 U.S. 347 (1967)
[20] ECHR. *Case of Halford v. The United Kingdom*. Judgment of 25 June 1997, application no. 20605/92; *Case of Rotaru v. Romania*. Judgment of 4 May 2000, application no. 28341/95; and *Case of P.G. and J.H. v. The United Kingdom*. Judgment of 25 September 2001, application no. 44787/98.
[21] Corte IDH. *Fontevecchia y D'Amico vs. Argentina*, supra nota 6.
[22] *U.S. v Jones* 10 U.S. 1259 (2011), J. Sotomayor concurring.
[23] Lo anterior sin perjuicio de que el registro de comunicaciones que prevé el artículo 44 fracción XII de la Ley Federal de Telecomunicaciones presenta serias deficiencias de constitucionalidad.

En este sentido, es claro que la obtención de datos de localización geográfica en tiempo real, de los equipos de comunicación móvil asociados a una línea que establece el Decreto, constituye una interferencia con el derecho a la privacidad y al derecho a la inviolabilidad de las comunicaciones privadas reconocido en el artículo 16 constitucional, párrafos primero, decimosegundo y decimotercero, el artículo 11 de la CADH y el artículo 17 del PIDCP.

Ahora bien, una vez que se ha determinado el contenido y alcance de la protección del derecho a la privacidad y el derecho a la inviolabilidad de las comunicaciones privadas y que la obtención de los datos de geolocalización constituyen una interferencia con esos derechos, es preciso recordar que los mismos pueden ser limitados. Como la Corte IDH ha señalado en su jurisprudencia:

> *"La fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. Este progreso […] no significa que las personas deban quedar en una situación de vulnerabilidad frente al Estado o a los particulares. De allí que el Estado debe asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada.*
>
> *No obstante conforme se desprende del artículo 11.2 de la Convención, el derecho a la vida privada no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias; por ello, deben estar previstas en ley, perseguir un fin legítimo y ser necesarias en una sociedad democrática".*[24]

De lo anterior se desprende que cualquier interferencia con el derecho a la privacidad debe cumplir con tres requisitos: 1) Legalidad 2) Persecución de un fin legítimo y 3) Necesidad en una sociedad democrática.

---

[24] Corte IDH. *Escher Vs, Brasil*, supra nota 11, párr. 116.

Especialmente cuando la medida restrictiva se refiere a técnicas de vigilancia que por su naturaleza son secretas, como la intervención de comunicaciones privadas o el monitoreo por geolocalización, los riesgos de arbitrariedad son evidentes, por lo que deben adoptarse medidas para evitar el abuso de esas facultades depositadas en el ejecutivo.[25] Por lo tanto, para que las disposiciones del Decreto puedan considerarse compatibles con la Constitución y los tratados internacionales en materia de derechos humanos, es indispensable que se ajusten al *test tripartito* mencionado en el párrafo anterior.

Legalidad

El requisito de legalidad implica que "las condiciones y circunstancias generales conforme a las cuales se autoriza una restricción al ejercicio de un derecho humano determinado deben estar claramente establecidas por ley. La norma que establece la restricción debe ser una ley en el sentido formal y material".[26]

A su vez en el contexto del derecho a la vida privada y el derecho a la inviolabilidad de las comunicaciones privadas, las medidas que restrinjan esos derechos deben ser precisas e indicar reglas claras y detalladas sobre la materia[27] tales como las circunstancias en que dicha medida puede ser adoptada; las personas autorizadas a solicitarla, a ordenarla y a llevarla a cabo; el procedimiento a seguir entre otros elementos.[28]

En el contexto de medidas encubiertas de vigilancia , como la geolocalización en tiempo real, la ley debe ser lo suficientemente clara en sus términos para otorgar a los ciudadanos una indicación adecuada respecto de las condiciones y circunstancias en que las autoridades están facultadas para recurrir a dichas

---

[25] ECHR. *Case of Weber and Saravia v. Germany*. Decision of 29 June 2006, application no. 54934/00 para. 93; *Case of Kennedy v. United Kingdom*. Judgment of 18 May 2010, application no. 26839/054 para. 152; and *Case of Malone v. United Kingdom*, supra nota 15 para. 67.
[26] Corte IDH. *La expresión "Leyes" en el artículo 30 de la Convención Americana sobre Derechos Humanos*. Opinión Consultiva OC-6/86 de 9 de mayo de 1986. Serie A. No. 6, párrs. 27 y 32; *Tristán Donoso Vs. Panamá,* supra nota 11, párr.. 77 y *Escher Vs. Brasil*, supra nota 11, párr. 130.
[27] Corte IDH. *Escher Vs. Brasil*, supra nota 11, párr. 131; ECHR. *Case of Kruslin v. France*. Judgment of 24 April 1990, application no. 11801/85, para. 33; *Case of Huvig v. France*. Judgment of 24 April 1990, application no. 11105/84, para. 32.
[28] Corte IDH. *Escher Vs. Brasil*, supra nota 11, párr. 131.

medidas.[29] Además, en vista del riesgo de abuso que cualquier sistema de vigilancia secreta implica, las medidas deben basarse en una ley que sea particularmente precisa, en vista de que la tecnología disponible para realizar esas actividades continuamente se vuelve más sofisticada.[30]

Adicionalmente, para que una medida que afecte el ámbito de protección del derecho a la inviolabilidad de las comunicaciones privadas pueda considerarse legal, es necesario que esta sea acorde a la garantía formal que establece de manera puntual el párrafo decimotercero del artículo 16 constitucional. En este sentido la medida necesariamente requiere que sea autorizada por la autoridad judicial federal, a petición de la autoridad competente la cual debe fundar y motivar su petición, indicando de manera clara y precisa, al menos, el tipo de medida, los sujetos de la misma y su duración.

Persecución de un fin legítimo

La medida que restrinja el derecho a la privacidad debe estar orientada a la persecución de un fin legítimo. El artículo 30 de la CADH señala como fines legítimos aquellos atinentes a la satisfacción de un interés general. Sin duda, la investigación y persecución de delitos, como parte del cumplimiento de las obligaciones positivas del Estado, son fines legítimos orientados a satisfacer un interés general como lo es la seguridad y el orden público.

Sin embargo no debe perderse de vista que las limitaciones deben responder exclusivamente a las "justas exigencias de una sociedad democrática, que tenga en cuenta el equilibrio entre los distintos intereses en juego"[31], por lo que de nuevo debe reiterarse que la utilización de medidas que restringen los derechos, en especial el derecho a la privacidad en el contexto del presente análisis, deben

[29] ECHR. *Case of Uzun v. Germany*, supra nota 16 para. 61; *Case of Malone v. United Kingdom*, supra nota 15 para. 67; *Case of Valenzuela Contreras v. Spain*, Judgment of 30 July 1998, application no. 58/1997/842/1048, para. 46.
[30] ECHR. *Case of Uzun v. Germany*, supra nota 16 para. 61; *Case of Weber and Saravia v. Germany*, supra nota 25 para. 93.
[31] Corte IDH. *La Colegiación Obligatoria de Periodistas.* Opinión Consultiva 0C-5/85 del 13 de noviembre de 1985, Serie A No. 6, párr. 38 y CIDH. *Informe sobre Seguridad Ciudadana y Derechos Humanos*. OEA/Ser.L/V/II. Doc. 57. 31 Diciembre 2009, párr. 174.

diseñarse con cuidado de no otorgar poderes ilimitados o que carezcan de medidas adecuadas que inhiban su abuso.

Necesidad en una sociedad democrática

Para que una medida que restringe el derecho a la privacidad pueda considerarse necesaria en una sociedad democrática esta debe ser idónea, necesaria *stricto sensu* y proporcional al fin legitimo perseguido. Especialmente en el contexto de medidas de vigilancia secreta, estas deben contemplar la adopción de medidas adecuadas y efectivas contra su abuso. Para determinar lo anterior en un caso concreto, deben valorarse la naturaleza, alcance y duración de las medidas, los motivos para su adopción, las autoridades competentes para autorizar, llevar a cabo y supervisar las medidas y las posibilidades para controvertir la medida o remediar los efectos de su adopción.[32] Para ello es indispensable analizar si los procedimientos diseñados para supervisar la compatibilidad de la solicitud, autorización e implementación de este tipo de medidas son suficientes para garantizar que la interferencia con el derecho a la vida privada se mantenga en línea con los requerimientos de que esta sea "necesaria en una sociedad democrática".[33]

Análisis del Decreto a la luz del test tripartito

Las disposiciones del Decreto en materia de geolocalización, en tiempo real, de los equipos de comunicación móvil, incumplen el requisito de legalidad y necesidad descritos en los párrafos anteriores, y generan graves riesgos de que la medida sea utilizada para fines distintos al fin legítimo de la persecución de delitos.

En primer lugar, resulta preocupante que el Decreto permita la obtención de datos de localización geográfica en tiempo real sin que previamente la autoridad tenga

[32] ECHR. *Case of Kennedy v. The United Kingdom*, supra nota 25 para. 153; *Case of Weber and Saravia v. Germany*, supra nota 25 para. 106; and *Case of Klass and others v. Germany.* Judgment of 6 September 1978, application no. 5029/71 para. 49-50.
[33] ECHR. *Case of Kennedy v. The United Kingdom*, supra nota 25 para. 154; and *Case of Kvasnica v. Slovakia*. Judgment of 9 June 2009, application no. 72094/01 para. 80.

que obtener una autorización por parte del poder judicial federal. Ese sólo hecho resulta suficiente para decretar la inconstitucionalidad del Decreto. La ausencia de una autorización judicial previa impide que en los casos concretos se garantice que la medida sea la idónea, necesaria y proporcional a la luz de una solicitud fundada y motivada por parte de la autoridad.

A su vez, en las disposiciones contenidas en el Decreto no se establece de manera clara, precisa y detallada las condiciones, el procedimiento y las personas respecto de las cuales puede llevarse a cabo la medida. Si bien, se limita la utilización de la medida a investigaciones relativas a los delitos de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas, no se establece el grado en el que una persona o un equipo de comunicación móvil deba estar relacionado con la investigación, es decir, no se establece si la existencia de una investigación sobre los delitos mencionados permite la obtención de datos de geolocalización de equipos de comunicación móvil que la autoridad investigadora, con base en distinto material probatorio, considere que puedan estar implicadas en la comisión de los delitos objeto de investigación o si la medida puede utilizarse para obtener datos de geolocalización de comunicación móvil asociadas a personas que no están involucradas de manera directa pero que la autoridad investigadora considere puedan ser útiles para la investigación.

De cualquier forma, en vista de que no existe un mecanismo de autorización judicial previo, de la obligación de sigilo y de la evidente secrecía de la medida, resulta imposible que exista la constatación de la debida fundamentación y motivación de la solicitud, sobre todo en tanto los permisionarios y concesionarios del servicio de telecomunicaciones poseen una estricta obligación de colaboración y su incumplimiento es fuertemente sancionado administrativa y penalmente.

A su vez, no se señala en la ley de manera clara, precisa y detallada otros elementos de la solicitud como la duración de la medida y el tratamiento de los datos producto del monitoreo. De la manera en que están redactadas las disposiciones del decreto, se permite a la PGR realizar el monitoreo a través de la obtención de datos de localización geográfica en tiempo real de manera indefinida, sin que

tampoco se detalle la forma en la que deba procesarse, tratarse, transmitirse o destruirse la información recabada mediante dicho monitoreo.

Tampoco resulta clara la existencia de recursos adecuados y efectivos para impedir y remediar las violaciones con motivo del abuso de la implementación de esta medida. Si bien se hace referencia a la fracción IV del artículo 214 del Código Penal Federal en relación a la utilización de los datos e información obtenidos como resultado de la localización geográfica de equipos de comunicación móvil para fines distintos a los estrictamente relacionados a las investigaciones objeto de la medida, lo cierto es que esa medida resulta insuficiente para prevenir y detectar y remediar las violaciones.

Lo anterior es claro, en tanto la medida por su propia naturaleza secreta, se encuentra fuera del conocimiento de la persona objeto de la interferencia y fuera del escrutinio público. Por ello es indispensable que existan mecanismos revisión independiente periódica o permanente de este tipo de mecanismos para evitar su abuso. En vista de la ausencia de cualquier tipo de control y supervisión a cargo de una autoridad judicial, parlamentaria o administrativa, resulta claro que no existen salvaguardas adecuadas para evitar el abuso de esta medida, por lo que se incumple el requisito de que las medidas resulten necesarias en una sociedad democrática.

En virtud de lo anteriormente señalado debe concluirse que el artículo 133 Quáter del Código Federal de Procedimientos Penales y los artículos 40 Bis y 44 fracciones XVI y XVII de la Ley Federal de Telecomunicaciones, relativas a la facultad de la autoridad investigadora para obtener los datos de geolocalización, en tiempo real, de equipos de comunicación móvil resultan violatorias de los artículos 16 de la Constitución, 11 de la CADH y 17 del PIDCP en relación con el artículo 1º Constitucional y los artículo 1.1 y 2 de la CADH y 2 del PIDCP.

A su vez, el artículo el artículo 178 Bis del Código Penal Federal y los artículos 3 fracción XVII, 71 apartado A fracción VI y artículos Transitorios Tercero y Cuarto de la Ley Federal de Telecomunicaciones contenidos en el Decreto también deben

ser considerados como inconstitucionales de manera residual a las disposiciones principales mencionadas en el párrafo anterior.

Por lo tanto resulta indispensable que la Comisión Nacional de los Derechos Humanos ejerza la facultad que le otorga el artículo 105 fracción II inciso g) de la Constitución e interponga una acción de inconstitucionalidad en contra de las disposiciones del Decreto mencionadas de manera que la Suprema Corte de Justicia de la Nación expulse dichas disposiciones del ordenamiento jurídico mexicano.

Comentarios Finales

Resulta importante resaltar que por la propia naturaleza secreta en la que estas disposiciones serían implementadas, resultaría sumamente difícil para la ciudadanía en general el combatir la abierta inconstitucionalidad de estas disposiciones, por ello la facultad que posee la CNDH para interponer acciones de inconstitucionalidad reviste una importancia especial para el cumplimiento de su obligación de protección de los derechos humanos.

La interposición de la acción de inconstitucionalidad además sería un precedente importante que debería conducir a orientar la actividad legislativa, las actuaciones ministeriales y la conducta judicial respecto de la importancia de salvaguardar el derecho a la vida privada en un entorno en el que la utilización de medidas tecnológicas invasivas reduce las capacidades de escrutinio público de la utilización de dichas medidas y por ende se incrementa la vulnerabilidad de los ciudadanos ante el comportamiento potencialmente arbitrario y abusivo de la autoridad.

Resulta fundamental que la CNDH asuma su papel de protección de los derechos humanos y rechace las falsa contradicción entre seguridad y derechos. Por el contrario, la interposición de la acción de inconstitucionalidad que en este análisis se recomienda representa una oportunidad para que se consolide la visión de que sólo a través del respeto, promoción, garantía y protección de los derechos

humanos es posible alcanzar los objetivos de una sociedad democrática y que la concesión de facultades discrecionales sin la adopción de pesos y contrapesos que inhiban el abuso de esas facultades es un camino que lejos de favorecer a la obtención de la paz y la seguridad fomentan la arbitrariedad, la cultura de ilegalidad y ponen en riesgo la seguridad y privacidad de la ciudadanía.