# LA INVESTIGACIÓN PENAL EN LA ERA DIGITAL. A PROPÓSITO DEL CASO CARPENTER *VS.* ESTADOS UNIDOS

Héctor Ivar Hidalgo Flores*

* Abogado. Estudiante de la Maestría en Juicio Oral del INACIPE.

## PALABRAS CLAVE *KEYWORDS*

| | |
|---|---|
| **Era digital** | *Digital age* |
| **Investigación penal** | *Criminal investigation* |
| **Privacidad** | *Privacy* |
| **Control judicial** | *Judicial control* |



**Resumen.** En la actualidad, las autoridades encargadas de la persecución penal han aprovechado la tecnología para crear nuevas técnicas de investigación que podrían poner en riesgo la privacidad de las personas. En este contexto, el presente trabajo examinará un caso relacionado con esta problemática. En Carpenter *vs.* Estados Unidos la Corte Suprema de los Estados Unidos analizó una de estas herramientas: el acceso a los registros de telecomunicaciones que permiten rastrear los lugares donde ha estado un teléfono celular. En este sentido, el presente estudio pretende identificar cuáles son los argumentos más significativos de este emblemático fallo, sobre todo aquellos que podrían ser utilizados en casos posteriores.

**Abstract.** At present, the authorities in charge of criminal prosecution have taken advantage of the technology to create new investigative techniques that could put people's privacy at risk. In this context, the present work will examine a case related to this problem. In Carpenter v. United States, the Supreme Court of the United States analyzed one of these tools: access to telecommunications records that allow tracking the places where a cell phone has been. In this sense, the present study aims to identify which are the most significant arguments of this important ruling, especially those that could be used in later ca risk ses.

SUMARIO:



## I. INTRODUCCIÓN

En la actualidad la tecnología ha permeado en prácticamente todas las actividades que realizamos. Por tanto, no es de extrañar que las autoridades también hayan echado mano de los avances de la ciencia. En el caso de las autoridades encargadas de la investigación penal, podemos decir que han actualizado de manera importante su repertorio de técnicas de investigación. En este momento, los órganos responsables de la persecución criminal cuentan con herramientas tecnológicas sumamente sofisticadas, las cuales no podríamos haber imaginado hace unos años.

De manera paralela, los Estados han tratado de regular las nuevas técnicas de investigación para evitar abusos por parte de los agentes estatales. En efecto, estas nuevas tecnologías pueden llegar a ser tan invasivas que podrían revelar cada uno de los aspectos de la vida privada de una persona. De ahí que la legislación, además de los órganos jurisdiccionales,[1] busquen ser contrapesos a estas nuevas herramientas de investigación.

Es en esta era digital que se inserta el caso que analizaremos. En Carpenter *vs.* Estados Unidos (2018) la Corte Suprema de los Estados Unidos (CS) resolvió una problemática singular: analizó si la autoridad lleva a cabo una inspección al acceder a los registros de telecomunicaciones que permiten rastrear los lugares en que ha estado un teléfono celular; en otras palabras, el Tribunal Supremo examinó si la autoridad, al acceder a estos datos conservados, afecta las expectativas de privacidad de las personas.

El presente análisis pretende identificar cuáles son los argumentos más significativos de este emblemático fallo, sobre todo aquellos que podrían ser utilizados en casos posteriores. Asimismo, en aras de hacer un ejercicio comparativo, se hará mención a la forma en que la legislación mexicana regula el acceso a este tipo de registros de telecomunicaciones.

[1] Al respecto, en Johnson *vs.* Estados Unidos (1948), el Tribunal Supremo señaló que las inferencias que justifican la emisión de una orden de inspección deben ser extraídas "por un independiente y neutral magistrado en lugar de ser juzgadas por el oficial comprometido en la [...] competitiva tarea de descubrir el crimen" (p. 14).

De esta forma, este trabajo comenzará con algunas precisiones sobre las técnicas que se utilizan en la investigación criminal, sobre todo para comprender en qué casos su aplicación constituye una inspección o registro. Posteriormente, entraremos de lleno a examinar el fallo del Tribunal Supremo. De esta forma, analizaremos la sentencia en el siguiente orden: las torres de telefonía celular, los hechos, la cuarta enmienda, ubicación y privacidad, la *third-party doctrine*, y los alcances de la decisión. Finalmente, haremos mención a la regulación mexicana en cuanto a los datos conservados.

## II. LAS INSPECCIONES EN LA INVESTIGACIÓN PENAL

Antes de entrar de lleno al análisis de la sentencia, es necesario hacer algunas precisiones sobre las inspecciones o registros que practica la autoridad investigadora cuando tiene conocimiento de un delito. En este sentido, debemos tener en cuenta que la CS, como preámbulo, se pregunta si el Estado lleva a cabo una inspección cuando accede a los registros de telecomunicaciones que permiten rastrear los lugares en que ha estado un teléfono celular. Esta pregunta es de vital importancia, ya que el determinar si realmente la autoridad practica una inspección cuando tiene acceso a dicha información trae diversas consecuencias.

Ahora bien, la CS cuenta con dos criterios para establecer si cierta técnica de investigación es una inspección a la luz de lo que dispone la cuarta enmienda. En un principio, la jurisprudencia del Tribunal Supremo era sumamente conservadora, ya que únicamente consideraba que existía un registro cuando la autoridad invadía físicamente un determinado lugar (Estados Unidos *vs.* Jones, 2012). Por ejemplo, en Olmstead *vs.* Estados Unidos (1928) resolvió que la intervención de comunicaciones telefónicas no constituía una inspección, toda vez que la policía no se había introducido al domicilio de Roy Olmstead —investigado por posesión, transporte y venta de alcohol durante la vigencia del *Volstead Act* (Ley Seca)— para recabar las conversaciones telefónicas.

Posteriormente la CS cambió este criterio rígido para determinar la existencia de un registro. En Katz *vs.* Estados Unidos (1967) donde se analizó la intervención de comunicaciones practicada sobre una cabina telefónica, el Tribunal Supremo resolvió que "la Cuarta Enmienda protege personas, no lugares" (p. 351), y expandió el alcance de la enmienda para proteger determinadas

expectativas de privacidad. Este es un salto importante en la jurisprudencia de la CS, ya que permite mantener vigente el contenido de la Constitución.

De esta manera, tenemos que el Tribunal Supremo entiende que existe una inspección si, por un lado, la autoridad lleva a cabo un allanamiento físico en determinado lugar y, por otro, si la autoridad vulnera determinadas expectativas de privacidad.

Sentado lo anterior, una vez que se ha establecido que cierta herramienta de investigación constituye un registro, la CS ha señalado que, por regla general, toda inspección, para que se considere razonable, debe estar precedida de una orden judicial (Vernonia School District 47J *vs.* Acton, 1995).

Finalmente, corriendo el riesgo de ser repetitivo, pero en aras de dar claridad a los siguientes apartados, tenemos que el Tribunal Supremo considera que existe una inspección o registro a la luz de la cuarta enmienda si la autoridad invade físicamente un determinado lugar o si se violan las expectativas de privacidad de la ciudadanía. Asimismo, tiene claro que, por regla general, toda inspección o registro debe estar precedido de una orden judicial.

## III. CARPENTER *VS.* ESTADOS UNIDOS. UN CASO EMBLEMÁTICO

### A. LAS TORRES DE TELEFONÍA CELULAR

Curiosamente, la CS no inicia el análisis de Carpenter *vs* Estados Unidos planteando los hechos del caso, sino que dedica un par de páginas (1 y 2) para enfatizar la importancia de la tecnología —en específico, la de las torres de telefonía celular—. De esta manera, comienza señalando un dato demoledor: "Existen 396 millones de cuentas de telefonía celular en los Estados Unidos (para una nación de 326 millones de personas)" (Carpenter *vs.* Estados Unidos, 2018, p. 1).[2] Posteriormente, el Tribunal Supremo precisa que los teléfonos celulares llevan a cabo sus funciones conectándose a un conjunto de antenas conocidas como torres de telefonía celular; estas torres —señala—, pueden ser encontradas en postes de luz, campanarios o en los costados de edificios (*idem*).[3]

[2] Esta importancia de la telefonía celular y de los dispositivos móviles ya la ha enfatizado al grado de señalar que los teléfonos celulares son "una importante característica de la anatomía humana" (Riley *vs.* California, 2014, p. 9).

[3] La CS solo señala unos ejemplos, ya que este tipo de tecnología ha invadido todo nuestro entorno. Al respecto, podemos decir que muchas

Además, establece que los teléfonos celulares continuamente están buscando la mejor señal para conectarse, la cual proviene, generalmente, de las torres de telefonía más cercanas (*idem*).

La CS precisa que los teléfonos celulares, sobre todo los teléfonos inteligentes, se conectan varias veces a la red inalámbrica, siempre que la señal del teléfono esté encendida, incluso cuando no se está utilizando ninguna característica del dispositivo (*ibidem*, pp. 1, 2). Posteriormente, menciona un aspecto importante de estas torres: este conjunto de antenas de telefonía celular genera un registro cada vez que un dispositivo móvil lleva a cabo una conexión inalámbrica (*ibidem*, p. 2).

El Tribunal Supremo señala que las compañías telefónicas almacenan estos registros para sus propósitos comerciales; por ejemplo, para encontrar lugares en que no haya conexión o para cobrar cargos extra de *roaming* cuando otra compañía se conecta a sus antenas (*idem*). Finalmente, en esta parte de la sentencia se precisa que los más modernos teléfonos celulares generan registros telefónicos con información detallada sobre la ubicación de una persona (*idem*).

Ahora bien, estas torres, como lo menciona la CS, generan un registro cada vez que un teléfono celular se conecta a ellas. Dicho registro se puede producir incluso cuando no se está utilizando ninguna característica del dispositivo móvil. Por lo que el registro, como se señala en la sentencia, puede generar información sobre la ubicación de una persona. Por ejemplo, si un usuario se conecta a determinada torre en cierta hora, esta torre, que cubre cierto espacio geográfico, puede dar una idea sobre el lugar en el que se encuentra una persona; de ahí la importancia de los registros que generan las torres de telefonía celular.

## B. LOS HECHOS

En 2011 la policía arrestó a cuatro personas bajo la sospecha de haber robado diversas tiendas de telefonía celular; uno de estos sospechosos confesó que, en los meses previos, junto con un grupo de personas, había robado nueve tiendas en Michigan y Ohio (*idem*). El sospechoso identificó a 15 sujetos que habían intervenido en los atracos y dio al FBI sus números telefónicos (*idem*).

Basados en esta información, los fiscales del caso solicitaron órdenes judiciales para obtener los registros

veces ni siquiera nos percatamos de la existencia de estas torres, toda vez que las empresas de telefonía celular las instalan utilizando el camuflaje. Así, podemos encontrar torres que simulan ser palmeras, cactus o cualquier otro tipo de ejemplar arbóreo (*vid*., Stromberg, 2015).

telefónicos de Timothy Carpenter, lo anterior al amparo del *Stored Communications Act*, ley que permite que la autoridad solicite determinados registros de telecomunicaciones, y únicamente exige que dicha información sea relevante para una investigación criminal. Estas órdenes fueron concedidas por dos jueces federales y se dirigieron a dos compañías telefónicas (*ibidem*, p. 3). En conjunto, las dos empresas entregaron alrededor de 129 días de registros telefónicos, los cuales significaban 12898 puntos de ubicación en los que había estado el teléfono de Carpenter. Este fue acusado de seis cargos de robo y de seis cargos por portación de arma de fuego durante un delito federal (*idem*). Antes del juicio Carpenter solicitó que los registros de ubicación fueran suprimidos, ya que no habían sido obtenidos mediante una orden judicial apoyada por el estándar probatorio conocido como *probable cause*;[4] la Corte de Distrito negó su petición (*idem*).

Posteriormente, en el juicio, siete de sus cómplices lo señalaron como el líder de los robos (*idem*). Adicionalmente, un agente del FBI ofreció testimonio experto sobre los registros de ubicación. El agente explicó que cada vez que un teléfono celular se conecta a una red inalámbrica genera un registro de ubicación. Con esta información, el agente del FBI produjo mapas que colocaban el teléfono de Carpenter cerca de cuatro de los robos perpetrados (*ibidem*, pp. 3, 4). En sus alegatos de clausura, la autoridad señaló que Carpenter estaba justo donde había sucedido el robo, y al mismo tiempo en que se produjo. Carpenter fue sentenciado a más de 100 años de prisión (*ibidem*, p. 4).

Finalmente, la Corte de Apelaciones para el Sexto Circuito confirmó esta sentencia, y precisó que Carpenter carecía de una razonable expectativa de privacidad, ya que los usuarios de telefonía celular voluntariamente transmiten los registros de ubicación a sus empresas de telecomunicaciones como condición para establecer comunicación; por tanto —concluyó—, dichos registros no se encuentran protegidos por la cuarta enmienda (*idem*).

## IV. LA CUARTA ENMIENDA EN LA ERA DIGITAL

### A. LA CUARTA ENMIENDA

La cuarta enmienda dispone lo siguiente:

[4] El cual, hay que añadir, es el requerido para obtener cualquier orden de inspección. Para un estudio sobre este estándar se puede ver Estados Unidos *vs*. Martinez-Fuerte (1976).

> El derecho de los habitantes a estar seguros en sus personas, domicilios, documentos y bienes contra inspecciones y confiscaciones irrazonables no se violará, y no se emitirán órdenes, sino por causa probable, respaldadas por juramento o protesta, y, en particular, describiendo el lugar que debe buscarse y las personas o cosas que se deben confiscar (Cuarta Enmienda, 1792).

En Carpenter *vs.* Estados Unidos la CS hace un repaso somero de los precedentes que han definido los contornos de esta enmienda. En un primer momento, el Tribunal Supremo establece que esta disposición pretende proteger a las personas contra invasiones arbitrarias de los agentes estatales (Carpenter *vs.* Estados Unidos, 2018, p. 4). Como se ha señalado con anterioridad, la jurisprudencia de la CS únicamente reconocía que existía una inspección cuando la autoridad invadía físicamente determinado lugar. En la sentencia se pone énfasis en que esta limitada visión se terminó cuando se resolvió el caso Katz, ya que en este asunto se estableció que la cuarta enmienda protege ciertas expectativas de privacidad (*ibidem*, p. 5).

La CS pone de relieve que la enmienda tutela las "intimidades de la vida" contra el "poder arbitrario" (*ibidem*, p. 6). Algo que hay que resaltar es que el Tribunal Supremo, refrendando el criterio establecido en Estados Unidos *vs.* Di Re (1948), tiene claro que el espíritu de esta disposición constitucional consiste en colocar obstáculos para evitar una permanente vigilancia policial (Estados Unidos *vs.* Carpenter, 2018, p. 6). Este es un aspecto medular del fallo que podría utilizarse en casos posteriores, ya que, como se verá a continuación, la duración de la técnica de investigación es un criterio para determinar si cierto acto de autoridad es una inspección.

Posteriormente, la CS trae a colación el caso Kyllo *vs.* Estados Unidos (2001); uno de los asuntos más fascinantes que ha resuelto. De este precedente podemos resaltar lo siguiente: en 1992, Danny Kyllo era investigado por cultivar plantas de marihuana en su domicilio. La policía utilizó un artefacto que genera imágenes térmicas, el cual dirigió a uno de los costados de la casa de Kyllo, sin contar con una orden judicial. Para entender mejor, y como se señala en Kyllo, para el cultivo de marihuana en interiores se utilizan lámparas de halógeno que producen grandes cantidades de calor; de ahí la intención de usar uno de estos dispositivos térmicos, ya que la policía buscaba detectar si existía calor excesivo al interior de la casa del sospechoso. Con base en la información proporcionada por este artefacto, y con los recibos de luz, se solicitó una orden de inspección

para ingresar a la casa de Kyllo, el cual, efectivamente, estaba cultivando plantas de marihuana.

En Carpenter (2018), la CS recuerda que la utilización de este aparato térmico constituyó una inspección; además, resalta que en Kyllo se rechazó una "interpretación mecánica" de la cuarta enmienda. Asimismo, se precisa que de haberse resuelto lo contrario se dejaría a la ciudadanía a merced de los avances tecnológicos. De la misma forma, la CS recuerda que en Kyllo se resolvió que el uso de este dispositivo térmico debía estar precedido de una orden judicial (pp. 6, 7).

Otro precedente que se invoca es el caso Riley *vs.* California (2014). En este importante asunto, la CS resolvió que la policía, por regla general no puede, sin una orden de inspección, acceder a la información digital de un teléfono celular que ha sido confiscado durante un arresto. De esta sentencia, el Tribunal Supremo recordó que la necesidad de esta orden se justifica por el hecho de que los teléfonos celulares contienen una enorme capacidad de almacenamiento (Carpenter *vs.* Estados Unidos, 2018, p. 7), lo cual —añadimos—, pone en riesgo la privacidad de las personas.

Ahora bien, de esta parte del fallo se desprende una interpretación evolutiva de la cuarta enmienda. Asimismo, algunos argumentos se refrendan y, por tanto, dan cabida a pensar que podrían ser utilizados posteriormente. Por ejemplo, los relativos a considerar que la duración de la técnica de investigación es un parámetro para determinar si nos encontramos ante un acto que podría considerarse una inspección y, en consecuencia, que vulnera la privacidad de una persona; o el argumento en el que se rechaza el uso de una interpretación mecánica o literal de la cuarta enmienda.

## B. UBICACIÓN Y PRIVACIDAD

En este apartado se revisarán los argumentos de la Corte en cuanto a la privacidad en la ubicación y en los movimientos de una persona. En la sentencia se van a tomar en cuenta, principalmente, dos precedentes. El primero se refiere al caso Estados Unidos *vs.* Knotts (1983), en el que se resolvió una problemática curiosa. Tristan Armstrong, un exempleado de una compañía que fabricaba químicos, comenzó a ser investigado por la policía de Minnesota bajo la sospecha de que estaba robando sustancias químicas que permitían fabricar drogas ilícitas. Investigaciones posteriores indicaron que esta persona también estaba comprando químicos a la empresa Hawkins Chemical. Posteriormente, aplicando una técnica

de investigación, la policía solicitó a esta compañía permiso para colocar un bíper dentro de un contenedor de cloroformo,[5] el cual Armstrong iba a adquirir. Los agentes de investigación utilizaron el bíper para rastrear el contenedor a través del tráfico. Primero, Armstrong lo entregó a Darryl Petschen, otro de los sospechosos; después, este lo llevó a la cabaña propiedad de Leroy Knotts en Wisconsin. Con base en esta información, los oficiales solicitaron una orden de inspección para acceder a la cabaña de Knotts, lo cual permitió descubrir que en ésta se encontraba funcionando un laboratorio para fabricar drogas ilícitas.

En Carpenter (2018), la CS resalta que en Knotts se concluyó que la vigilancia visual realizada con apoyo de un bíper no constituía una inspección, ya que una persona viajando en un automóvil por la vía pública no tenía una razonable expectativa de privacidad en sus movimientos. Otro argumento rescatado fue el relativo a que se debe distinguir entre el rudimentario rastreo realizado con un bíper durante un breve viaje automovilístico y otras formas de vigilancia que pudieran durar 24 horas (pp. 7, 8). Como vemos, en Knotts, la CS tuvo en cuenta el parámetro temporal para determinar si cierta técnica de investigación podría vulnerar la privacidad de las personas. En este sentido, fue cuidadosa en dejar la puerta abierta ante otro tipo de actos de investigación más prolongados.

Pues bien, el otro precedente utilizado en esta parte de la sentencia es Estados Unidos *vs.* Jones (2012). En este caso se resolvió que el Estado, al colocar un dispositivo GPS en un vehículo para monitorear sus movimientos, llevaba a cabo una inspección. Ahora bien, se ha considerado que este precedente es un retroceso en la jurisprudencia de la CS, ya que en él se vuelve a realizar una interpretación mecánica o rígida de la cuarta enmienda, toda vez que se determinó que se vulneraba esta disposición constitucional debido a una intrusión física, y no en virtud de que se violaran las expectativas de privacidad de una persona. Realmente no se sostiene esta crítica, debido a que la propia enmienda habla de que los "bienes" de una persona se encuentran protegidos de inspecciones y confiscaciones irrazonables. De ahí que la CS no haya tenido otra opción que resolver de la forma en que lo hizo.

Respecto al caso Jones, el Tribunal Supremo destacó que en los votos concurrentes se señaló que las expectativas de privacidad de una persona se verían en riesgo

[5] Un llamado "precursor" para fabricar drogas ilícitas (Estados Unidos *vs.* Knotts, 1983, p. 278).

si se permitía que la autoridad, con el apoyo de un GPS, rastreara un vehículo por un tiempo prolongado, independientemente de que estos movimientos se hicieran públicamente (Carpenter *vs.* Estados Unidos, 2018, pp. 8, 9). Como vemos, con este razonamiento se trata de atemperar lo señalado en Knotts, en el sentido de que una vigilancia prolongada sobre determinados movimientos físicos, no importando que los mismos se hagan en público, puede considerarse como violatoria del derecho a la privacidad.

Para desvirtuar los argumentos en el sentido de que el acceso a los registros de telecomunicaciones no constituye una inspección, la CS señala que una persona no renuncia a la protección de la cuarta enmienda por incorporarse a la esfera pública. Citando a Katz, establece que "lo que una persona busca preservar como privado, incluso en un lugar accesible al público, puede estar constitucionalmente protegido" (*ibidem*, p. 12). La CS establece que permitir el acceso a los registros de telecomunicaciones vulnera las expectativas de privacidad de una persona. Para justificar lo anterior, señala que el rastrear la ubicación de un teléfono celular por un tiempo prolongado puede evidenciar información exhaustiva sobre el paradero de una persona, por ejemplo, puede revelar no solo determinados movimientos sino sus inclinaciones familiares, políticas, religiosas e, incluso, sexuales (*idem*). La utilización de los registros de telecomunicaciones puede ser más invasivo que el GPS de Jones o el bíper de Knotts, ya que estos registros digitales rastrean cada uno de los movimientos del usuario de un teléfono celular. La CS desvirtúa el argumento que señala que los registros de telecomunicaciones son menos precisos que el GPS (*ibidem*, pp. 13, 14). Al respecto, reitera lo que se dijo en Kyllo, en el sentido de que los avances de la tecnología van a mejorar esta precisión (*ibidem*, p. 14). Finalmente, la CS concluye esta parte de la sentencia señalando que el acceso a los registros de ubicación vulneró las expectativas de privacidad de Carpenter (*ibidem*, p. 15).

De este apartado podemos rescatar los argumentos relativos a que una vigilancia policial prolongada puede considerarse violatoria del derecho a la privacidad. Además, llama la atención uno de los razonamientos torales de la CS: el relativo a que una persona no renuncia a la protección de la cuarta enmienda, es decir, a la protección de su privacidad, por el hecho de incorporarse a la esfera pública. En un pasaje de la sentencia, el Tribunal Supremo pone énfasis en que sólo los pocos que no cuenten con un teléfono celular podrían escapar de

esta incansable y absoluta vigilancia (*ibidem*, p. 14). Lo anterior enfatiza el hecho de que la CS trata de realizar una interpretación constitucional que atienda las circunstancias actuales en que vivimos.[6] Resultaría totalmente absurdo que el Tribunal Supremo se mantuviera anclado en un entendimiento literal de la Constitución. Pensemos que se tuviera que dejar de usar el teléfono celular para evitar la vigilancia estatal. Lo anterior impediría la utilización de la tecnología, además de que no se mantendría vigente el grado de protección que proporcionaba la cuarta enmienda cuando fue adoptada. En otras palabras: la CS entiende que no por usar un teléfono celular se renuncia al derecho a la privacidad, máxime cuando un teléfono móvil ya no es un simple accesorio, sino, como se mencionó en Riley (2014), "es una importante característica de la anatomía humana" (p. 9).

## C. LA *THIRD-PARTY DOCTRINE*

Para explicar la *third-party doctrine*, la CS también utiliza dos precedentes: Estados Unidos *vs.* Miller (1976) y Smith *vs.* Maryland (1979). En el primer caso, al estar investigando a Miller por evasión fiscal, la autoridad requirió a sus bancos que proporcionaran diversos cheques cancelados, depósitos y estados de cuenta. La CS resolvió que no existía una violación a la cuarta enmienda debido a que esta información bancaria no constituía una comunicación confidencial, sino documentos utilizados en las transacciones comerciales, además de que los registros bancarios contenían información expuesta a los empleados del banco en el curso ordinario de las operaciones. Por tanto, la CS concluyó que Miller había tomado el riesgo, al revelar su información bancaria a terceros, de que dicha información podría ser transmitida por estos terceros a la policía.

Por su parte, en Smith (1979), el Tribunal Supremo analizó el uso de un dispositivo (*pen register*) que permitía grabar los números marcados desde una línea telefónica fija. En este asunto, la CS señaló que cuando Smith marcaba un número, él mismo transmitía los números utilizados a la compañía telefónica. Por tanto, reiterando lo que señaló en Miller, Smith tomaba el riesgo de que dicha información podría ser transmitida a la policía.

Para dar mayor claridad, podemos decir que estos dos precedentes

[6] Algo parecido sucede con los tribunales regionales de derechos humanos. Por ejemplo, el Tribunal Europeo de Derechos Humanos ha considerado que el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales es un "instrumento vivo" que debe ser interpretado a la luz de las condiciones actuales (Tyrer *vs.* Reino Unido, 1978, párr. 31).

son los creadores de la *third-party doctrine*.[7] Esta doctrina, según se desprende de estos dos asuntos, se podría entender en el sentido de que cuando una persona transmite determinada información a un tercero, renuncia, por así decirlo, a la privacidad sobre dichos datos.

El argumento al cual se enfrentó la CS fue el relativo a que los registros de telecomunicaciones, al ser transmitidos a la compañía telefónica al aceptar usar un teléfono celular, ya no eran privados, sino que constituían simples registros generados en operaciones comerciales; es decir, que en Carpenter operaba la *third-party doctrine*.

En un principio, el Tribunal Supremo menciona que no se puede comparar la información transmitida en Miller y en Smith —es decir, información bancaria y números telefónicos marcados— con la exhaustiva cantidad de datos que proporcionan los registros de telecomunicaciones. La CS señala que el Estado no está pidiendo una aplicación rígida de la *third-party doctrine*, sino lo que solicita es que se aplique de manera extensiva a una categoría distinta de información (Carpenter *vs*. Estados Unidos, 2018, p. 15).

El Tribunal Supremo entiende que una persona tiene una reducida expectativa de privacidad en información que ha compartido con otros; pero la CS pone énfasis en que el hecho de que se reduzca esta privacidad no quiere decir que desaparezca (*ibidem*, pp. 15, 16). Lo anterior es a lo que nos referimos cuando aseveramos que no por el hecho de usar un teléfono celular se renuncia al derecho a la privacidad.

Pues bien, el Tribunal Supremo tiene claro que para que opere la *third-party doctrine* se debe tomar en cuenta la información que se comparte. La CS pone énfasis en que el caso se refiere a información detallada sobre la ubicación de una persona, compilada día a día, durante varios años (*ibidem*, pp. 16, 17). El Tribunal Supremo pone de relieve que no existe un consentimiento

[7] Adelantándonos un poco en nuestro estudio, podemos decir que esta doctrina podría servir a la Suprema Corte mexicana para adoptar una postura, ya que el Tribunal Constitucional se encuentra en la encrucijada de resolver si el acceso a la información bancaria requiere una orden judicial. En efecto, hace poco la Primera Sala de la Suprema Corte analizó el amparo directo en revisión 502/2017, en el cual se estableció que el entonces artículo 117, fracción II, de la Ley de Instituciones de Crédito era inconstitucional por vulnerar el derecho a la privacidad al permitir que el Ministerio Público local accediera a información financiera sin contar con una orden judicial. En el amparo directo en revisión 1762/2018, la Primera Sala pretendía reiterar este criterio al analizar la constitucionalidad del artículo 142, fracción I, de la Ley de Instituciones de Crédito. No obstante, el proyecto público generó gran polémica. En consecuencia, el 15 de agosto de 2018, la Primera Sala retiró el asunto para remitirlo al Pleno de la Suprema Corte. La Corte deberá ser muy cuidadosa en la resolución que emita, ya que el acceso a la información bancaria es una poderosa técnica de investigación. Además, deberá tener en cuenta todos los procesos que se encuentran en trámite, en los cuales, en muchos casos, se ha obtenido dicha información sin una orden judicial.

explícito del usuario de telefonía celular para que se generen los registros de telecomunicaciones (*idem*), los cuales se producen, como ya se mencionó, simplemente con que el teléfono esté encendido. Finalmente, la CS rechaza aplicar la *third-party doctrine*, ya que desde ningún punto de vista se puede decir que el usuario tome el riesgo de que los registros de telecomunicaciones sean transmitidos a un tercero; por tanto —concluye—, el acceso a estos registros es una inspección (*ibidem*, p. 17).

De este apartado se rescata el hecho de que la CS reitera que la información digital puede revelar todos los aspectos privados de la vida de una persona. Esto ya lo había precisado en Riley (2014) al señalar que los teléfonos celulares pueden almacenar grandes cantidades de información que revelan gran parte de la vida privada de una persona. Este criterio seguramente podría ser aplicado en casos posteriores. No obstante, como se verá a continuación, la CS limitó en gran medida los alcances de la decisión.

## D. ALCANCES DE LA DECISIÓN

Pues bien, la CS acotó de gran manera el alcance de Carpenter. En efecto, el Tribunal Supremo precisa que la sentencia es limitada, y que no existe un pronunciamiento sobre otras técnicas de investigación, como el uso de cámaras de vigilancia (Carpenter *vs.* Estados Unidos, 2018, pp. 17, 18). La CS señala que, al haber encontrado que la obtención de los registros telefónicos de Carpenter constituía una inspección, la autoridad debe, por regla general, contar con una orden judicial para acceder a dichos registros (*ibidem*, p. 18).

La CS pone énfasis en que no se puede obtener una orden judicial de acceso a los registros bajo el estándar requerido por la *Stored Communications Act*, es decir, por el mero hecho de que sean relevantes para una investigación. Para la obtención de un mandamiento judicial se requerirá acreditar el nivel probatorio conocido como *probable cause* (*ibidem*, pp. 18, 19). La CS es cuidadosa al señalar que existen casos excepcionales en que no se necesitará una orden para acceder a los registros de telecomunicaciones, como cuando se pretenda evitar amenazas contra personas, para prevenir la destrucción de evidencias o para evitar la fuga de una persona (*ibidem*, pp. 21, 22). El Tribunal Supremo cierra con una cita categórica. Al respecto, invoca al *justice* Brandeis, y precisa que la CS "está obligada [...] a garantizar que el progreso de la ciencia no erosione la

protección de la Cuarta Enmienda" (*ibidem*, p. 22).

No obstante que la CS limite en gran medida el fallo, del mismo se pueden desprender, como se ha venido señalando, diversos criterios generales que podrían ser utilizados en casos posteriores. Se entiende la pretensión de que el precedente sea limitado, ya que no se quiere correr el riesgo de entorpecer la persecución criminal. Sin embargo, como se mencionó, existen parámetros claros que podrían aplicarse en asuntos futuros que resuelva la propia CS o las demás cortes federales.[8]

## V. LA REGULACIÓN DE LOS DATOS CONSERVADOS. EL CASO MEXICANO

La obtención de los datos conservados se encuentra establecida en el Código Nacional de Procedimientos Penales. En la parte que nos interesa, este código precisa lo siguiente:

> **Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados**
>
> Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente.
>
> [...]
>
> Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el

[8] De hecho, esto ya sucedió. Inmediatamente después de que se emitió Carpenter, en junio pasado, la Corte de Apelaciones para el Séptimo Circuito resolvió un fascinante asunto aplicando algunos de los parámetros de la CS. En Naperville Smart Meter Awareness *vs.* Ciudad de Naperville (2018), esta corte concluyó que el servicio público de electricidad que proporciona la Ciudad de Naperville llevaba a cabo una inspección al acceder a un medidor digital que conservaba, de manera detallada, los datos sobre el consumo eléctrico de los habitantes de Naperville; en específico, los peticionarios se quejaron de que la información a la que accede el Estado puede dar una idea de si las personas se encuentran en casa, si están despiertas, si se encuentran cocinando, o si están cargando su carro eléctrico; al respecto, citando a Carpenter, la Corte de Apelaciones señaló que los residentes de Naperville, al estar obligados a usar el servicio público de electricidad, no asumen voluntariamente el riesgo de que su información de consumo sea transmitida a terceros; por tanto, determinó que no operaban Miller y Smith (p. 9).

> objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria. A partir de que se haya cumplimentado el requerimiento, el Ministerio Público deberá informar al Juez de control competente por cualquier medio que garantice su autenticidad, dentro del plazo de cuarenta y ocho horas, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación (Código Nacional de Procedimientos Penales, 2014, art. 303).

De lo anteriormente citado, aunque no se mencione de manera explícita, se puede entender que dentro de estos datos conservados se encuentran los registros de telecomunicaciones que permiten rastrear los lugares en que ha estado un teléfono celular, ya que son los que comúnmente resguardan los concesionarios. Como podemos ver, el artículo diseña un control judicial *ex ante* y uno *ex post* según existan circunstancias apremiantes o no, pero, por regla general, tenemos que el acceso a los datos conservados debe estar precedido de una orden judicial.

Hay que recordar que este artículo, en su redacción anterior, fue impugnado por la Comisión Nacional de los Derechos Humanos y por el Instituto Federal de Acceso a la Información Pública y Protección de Datos. En la emblemática acción de inconstitucionalidad 10/2014 y su acumulada 11/2014, la Suprema Corte de Justicia de la Nación resolvió que el control judicial previo es un verdadero derecho humano. En este asunto se analizó la figura de la localización geográfica en tiempo real. No obstante, esta figura comparte muchas características con la entrega de datos conservados, por lo que podría considerarse que lo resuelto en este caso también podría extenderse a los citados datos. Pues bien, la Suprema Corte, invocando la acción de inconstitucionalidad 32/2012, sorprendentemente resolvió que la citada localización geográfica en tiempo real, consagrada en la anterior redacción del artículo 303 del Código Nacional, no vulneraba el derecho a la privacidad. Sin embargo, estableció que el precepto era inconstitucional debido a que dicha localización geográfica en tiempo real, en su regulación anterior, no estaba limitada para la investigación de delitos específicos, sino que

se trataba de una facultad completamente abierta.

Resulta totalmente desafortunado que la Suprema Corte haya resuelto de esta manera, no importando que haya declarado, un poco de manera forzada, la inconstitucionalidad del precepto impugnado, ya que dejó incólume lo resuelto en la acción de inconstitucionalidad 32/2012, donde, como señalamos, se estableció que la localización geográfica en tiempo real no vulnera el derecho a la privacidad. Por todo lo que se ha dicho en este trabajo, es claro que esto no es así. El problema vendrá después, cuando se impugne el actual contenido del artículo 303 del Código Nacional de Procedimientos Penales, ya que este precepto, como se señaló, permite que el Ministerio Público, sin orden judicial previa, solicite la localización geográfica en tiempo real o, añadimos, los datos conservados. En este sentido, la Suprema Corte corre el riesgo de volver a establecer que esta técnica de investigación no vulnera el derecho a la privacidad, con lo cual se estaría reiterando un criterio que en la actualidad no se justifica.

## VI. CONCLUSIONES

No obstante que la CS limite en gran medida el fallo, del mismo se pueden desprender, como se ha precisado, diversos parámetros generales que podrían ser utilizados en casos posteriores. En un principio, tenemos que el Tribunal Supremo considera que existe una inspección o registro a la luz de la cuarta enmienda si la autoridad invade físicamente un determinado lugar o si se violan las expectativas de privacidad de las personas. Asimismo, tiene claro que, por regla general, toda inspección o registro debe estar precedido de una orden judicial.

Por otro lado, al referirse a la cuarta enmienda, el Tribunal Supremo reconoce que esta disposición constitucional pretende proteger a las personas contra invasiones arbitrarias de los agentes estatales, además tiene claro que su espíritu consiste en colocar obstáculos para evitar una permanente vigilancia policial. Asimismo, al analizar el caso, la CS rechaza una "interpretación mecánica" de la cuarta enmienda; además, precisa que de hacerse esta interpretación literal se dejaría a la ciudadanía a merced de los avances tecnológicos.

Al hablar sobre la ubicación y privacidad, el Tribunal Supremo establece que se debe distinguir entre el rudimentario rastreo realizado con un bíper durante un breve viaje automovilístico y otras formas de vigilancia que pudieran durar 24 horas. De esta manera, resuelve

que las expectativas de privacidad de una persona se verían en riesgo si se permitiera que la autoridad, con el apoyo de un GPS, rastreara un vehículo por un tiempo prolongado, independientemente de que estos movimientos se hicieran públicamente.

El Tribunal Supremo establece que no se puede comparar la información bancaria y los números telefónicos marcados con la exhaustiva cantidad de datos que proporcionan los registros de telecomunicaciones; asimismo, entiende que si bien una persona tiene una reducida expectativa de privacidad en información que ha compartido con otros, pone énfasis en que el hecho de que se reduzca esta privacidad no quiere decir que desaparezca; el Tribunal Supremo tiene claro que para que opere la *third-party doctrine* se debe tomar en cuenta la información que se comparte; la CS pone de relieve en que el caso Carpenter se refiere a información detallada sobre la ubicación de una persona, compilada día a día, durante años.

La CS pone énfasis en que no existe un consentimiento explícito del usuario de telefonía celular para que se generen los registros de telecomunicaciones, los cuales se producen cuando el teléfono está encendido. Finalmente, la CS rechaza aplicar la *third-party doctrine*, ya que desde ningún punto de vista se puede decir que el usuario tome el riesgo de que los registros de telecomunicaciones sean transmitidos a un tercero.

Finalmente, la obtención de datos conservados encuentra su regulación en el Código Nacional de Procedimientos Penales. No obstante que exista un marco legal, resulta desafortunada la interpretación que la Suprema Corte mexicana ha hecho del mismo, en el sentido de que el acceso a la localización geográfica en tiempo real, y añadimos, a los datos conservados, no vulnera el derecho a la privacidad.

## VII. FUENTES DE CONSULTA

### JURISPRUDENCIA

Corte de Apelaciones para el Séptimo Circuito. Naperville Smart Meter Awareness *vs.* Ciudad de Naperville. Núm. 16-3766. Resuelto el 16 de agosto de 2018.

Corte Suprema de Estados Unidos. Carpenter *vs.* Estados Unidos. 585 U.S. (2018). Slip Opinion. Resuelto el 22 de junio de 2018.

_____. Estados Unidos *vs.* Di Re. 332 U.S. 581. (1948). Resuelto el 5 de enero de 1948.

_____. Estados Unidos *vs.* Miller. 425 U.S. 435. (1976). Resuelto el 21 de abril de 1976.

_____. Estados Unidos *vs.* Martinez-Fuerte. 428 U.S. 543. (1976). Resuelto el 6 de julio de 1976.

_____. Estados Unidos *vs.* Knotts. 460 U.S. 276. (1983). Resuelto el 2 de marzo de 1983.

_____. Estados Unidos *vs.* Jones. 565 U.S. 400. (2012). Resuelto el 23 de enero de 2012.

_____. Johnson *vs.* Estados Unidos. 333 U.S. 10. (1948). Resuelto el 2 de febrero de 1948.

_____. Katz *vs.* Estados Unidos. 389 U.S. 347. (1967). Resuelto el 18 de diciembre de 1967.

_____. Kyllo *vs.* Estados Unidos. 533 U.S. 27. (2001). Resuelto el 11 de junio de 2001.

_____. Olmstead *vs.* Estados Unidos. 277 U.S. 438. (1928). Resuelto el 4 de junio de 1928.

_____. Riley *vs.* California. 573 U.S. (2014). Slip Opinion. Resuelto el 25 de junio de 2014.

_____. Smith *vs.* Maryland. 442 U.S. 735. (1979). Resuelto el 20 de junio de 1979.

_____. Vernonia School District 47J *vs.* Acton, 515 U.S. 646. (1995). Resuelto el 26 de junio de 1995.

Suprema Corte de Justicia de la Nación. Acción de inconstitucionalidad 32/2012. Resuelta el 16 de enero de 2014.

_____. Acción de inconstitucionalidad 10/2014 y su acumulada 11/2014. Resuelta el 22 de marzo de 2018.

_____. Amparo directo en revisión 502/2017. Resuelto el 22 de noviembre de 2017.

_____. Amparo directo en revisión 1762/2018. Pendiente de resolución.

Tribunal Europeo de Derechos Humanos. Tyrer *vs.* Reino Unido. Resuelto el 25 de abril de 1978.

## LEGISLACIÓN

Código Nacional de Procedimientos Penales. Publicado en el *Diario Oficial de la Federación* el 5 de marzo de 2014. Última reforma 17 de junio de 2016.

Cuarta Enmienda a la Constitución de los Estados Unidos. Adoptada el 1 de marzo de 1792.

## HEMEROGRAFÍA

Stromberg, J. (19 de abril de 2015). "The bizarre history of cellphone towers disguised as trees", en *Vox*. Recuperado el 30 de agosto de 2018 de https://www.vox.com/2015/4/19/8445213/cellphone-towers-trees.