La geolocalización como medio de prueba

Elisa Palomino Ángeles*
Amir García Villalpando**

Resumen:

Con el incremento de la utilización de los sistemas de posicionamiento global (GPS), se origina, en algunos supuestos jurídicos, la vulneración de ciertos derechos fundamentales. En las controversias judiciales, los referidos sistemas aportan elementos materiales, datos y medios de prueba, los cuales integran la prueba pericial en informática forense. Este artículo pretende determinar si es posible tener la exacta localización de un presunto imputado, con un sistema de posicionamiento global de alta calidad, para que la geolocalización sea precisa y pueda ser idónea como prueba, eliminando los riesgos tecnológicos en la operatividad de los GPS.

Abstract:

With the increase in the use of global positioning systems (GPS), originates, in some legal cases, the violation of some fundamental rights. In judicial disputes, the aforementioned systems provide material elements, data and means of proof, which integrate the expert evidence in computer forensics. This article aims to determine if it is possible to have the exact location of an alleged defendant, with a high-quality global positioning system, so that the geolocation is precise, and can be suitable as evidence, eliminating technological risks in the operation of GPS.

* Doctora en Derecho por la UNAM, Profesora-Investigadora del Departamento de Derecho, UAM-A., miembro de la Academia Mexicana de Ciberseguridad y Derecho Digital (AMCID) y de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI).

** Maestro en Estudios Urbanos por la UAM-A. y Maestro en juicios orales por la UNAM, Profesor-Investigador del Departamento de Derecho, UAM-A.

Introducción

En nuestros días, se ha incrementado el uso de los sistemas de posicionamiento global (GPS); consideramos que se debe, principalmente, a la inseguridad que percibe la ciudadanía común; esto trae consigo la probable vulneración de algunos derechos fundamentales, entre estos, el derecho a la privacidad en algunos supuestos jurídicos, así como la libertad, la seguridad jurídica y nacional, el uso y tratamiento indebidos de datos personales. Por ello, para intentar contrarrestar la inseguridad jurídica, algunas personas han optado por utilizar los instrumentos tecnológicos, tales como los rastreadores GPS, los cuales ayudan a localizar tanto a personas como a objetos.

Las tecnologías de rastreo, en las cuales se da un seguimiento con el teléfono móvil vía Internet y/o vía satelital, han originado supuestos jurídicos que anteriormente no se hubieran pensado; como ejemplo, el seguimiento de un fraude informático o la detención en flagrancia a través de una búsqueda del sujeto activo que cometió un hecho delictivo. Todas estas herramientas tecnológicas ponen al derecho en un debate sobre la obligación del Estado de investigar delitos y garantizar la seguridad jurídica en los casos en los que se utilizan los GPS como elementos materiales de la prueba pericial en materia de informática, así como el margen de error existente en la geolocalización con la tecnología actual, la necesidad de que la geolocalización sea más precisa para tener mayor certeza jurídica y cómo se debe incorporar este tipo de pruebas en los juicios orales.

Los elementos que la prueba pericial en informática forense requiere para los supuestos de la geolocalización, como el origen o la fuente de origen de la prueba, el contenido del soporte, en nuestro caso tecnológico, la relevancia jurídica y la licitud de la obtención de ella son requisitos que deben cumplirse para poder acreditar si un sujeto activo que, presuntamente, comete un hecho delictivo puede o no ubicarse a través de los GPS.

I. Los sistemas de posicionamiento global (GPS), conceptos, tipos y funciones

En la geolocalización opera un conjunto de elementos, entre ellos, el GPS, el cual "(…) es un servicio propiedad de los EE. UU., que proporciona a los

usuarios información sobre posicionamiento, navegación y cronometría. Este sistema está constituido por segmento del usuario. La fuerza Aérea de los Estados Unidos desarrolla, mantiene y opera el segmento espacial y el segmento de control".[1] En ese orden de razones, vamos a establecer lo siguiente:

a) Conceptos jurídico y técnico a nivel internacional y nacional

A los GPS también se les conoce como localización geográfica en el tiempo real; se entiende como "la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada".[2]

La connotación es diferente a lo que tradicionalmente conocemos como geolocalización, dentro de los elementos que se deducen de la definición tenemos: *a*) la ubicación aproximada en el momento de la búsqueda, *b*) la búsqueda de un equipo terminal móvil, y *c*) una línea telefónica determinada.

Destacamos que la ubicación de un equipo terminal móvil será aproximada, y no precisamente la del sujeto activo de un posible delito, porque sólo ubicaremos al equipo de una manera aproximada, lo que dará poca incertidumbre jurídica respecto a la temporalidad del hecho jurídico, y más tratándose de materia penal en la cual se requiere tener una certeza jurídica: "Esta figura de la geolocalización origina que las personas puedan ser ubicadas en un país, región que tiene más alta precisión (95-99%) en cuanto que la localización de la ciudad podría ser un poco menos preciso (50%). La identificación de la ubicación exacta del usuario, como el código postal/número construir es mucho menos preciso".[3] Lo referido depende del avance tecnológico del dispositivo móvil para determinar si podemos ubicar a la persona, como en el caso de los brazaletes electrónicos.

Asimismo, tenemos un concepto técnico que menciona:

> La geolocalización basada en IP representa la asignación de una determinada dirección IP de un dispositivo informático conectado a Internet o dispositivo móvil a su ubicación geográfica mundial. Geolocalización utiliza asignación de direcciones IP a: país, región

1 Gps.gov., "El sistema de posicionamiento global".
2 Instituto Federal de Telecomunicaciones, "Glosario".
3 Miip.org., "Geolocalización IP y dominios".

> o ciudad, latitud/longitud, ISP, nombre de dominio, etcétera" (Geolocalización IP y dominios).

En ese orden de ideas, tenemos que a nivel internacional se mencionan los datos de localización, y estableciendo otra connotación diferente a las que hemos referido, en la Directiva 2002/58/CE (Directiva sobre la Privacidad y las Comunicaciones Electrónicas) de la Comunidad Europea se hace mención de lo siguiente:

> Art. 2 inciso c), "(…) datos de localización" cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicación electrónica que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponibles para el público" (Diario oficial de la Unión Europea. Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009).

Por lo que se deduce que para la geolocalización o localización geográfica se requieren dos elementos: 1) la ubicación geográfica del equipo terminal de algún usuario, y 2) un servicio de comunicación electrónica disponible para el público y la monitorización constante del equipo terminal.

En México, en la Ley Federal de Telecomunicaciones y Radiodifusión,[4] en el artículo tercero fracción XXXV, se define la localización geográfica en tiempo real como: "Es la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada".

Los dispositivos móviles han venido a cambiar las formas en la cuales nos comunicamos y la manera en que nos localizan; el lenguaje hoy se comunica más con imágenes y con la escritura; la comunicación digital construye hoy en día la difusión de la opinión pública en la cual se envían discursos que crean fama o destruyen figuras políticas y culturales; con esta se hacen denuncias, juicios erróneos y correctos, juicios sumarios que condenan; también se puede informar o desinformar, se promueven estereotipos, o bien, se localiza o desubica a las personas que utilizan esos dispositivos móviles en un territorio de un Estado. En este aspecto, abordaremos una serie de impli-

[4] Ley Federal de Telecomunicaciones y Radiodifusión, artículo 3, fracción XXXV.

caciones jurídicas de los GPS como prueba pericial. En la geolocalización, necesariamente nos referirnos al elemento del territorio en el Estado-Nación, y en demás Estados, y guarda una relación entre el concepto de territorio y extraterritorialidad.

b) Tipos de modelos GPS

Existe una diversidad de sistemas de posicionamiento global con tecnologías de punta u obsoletas; son estos sistemas tecnológicos los que nos aportaran los soportes de almacenamiento y los elementos digitales que se encuentran contenidos en los referidos soportes. Los niveles de calidad de los GPS determinarán si la prueba pericial podrá ser eficaz para ubicar el lugar exacto en el cual se encuentra el dispositivo digital del sujeto activo de la conducta presuntamente delictiva; así como, dependiendo de la tecnología de punta, ubicar a la persona en tiempo real en algunos casos, no en todos, porque dependerá si cuenta con biometrías el dispositivo que se usa; razón por la cual, si alguna tecnología es más avanzada, se obtendrán datos más precisos.

Ahora bien, existen los tipos de GPS siguientes:

GPS1: Es un GPS personal, el cual funciona sobre la base de la red existente GSM/GPRS y los satélites GPS; este producto puede localizar y realizar el seguimiento de posibles objetivos a distancia por SMS o Internet.[5] Este sistema es usado tanto por los civiles como por los militares; los servicios pueden ser en satélite gratuitos o bien en Internet de paga.

GPS2: Es un GPS para vehículos. De igual manera funciona con red existente GSM/GPRS y los satélites GPS. Este producto puede localizar y realizar el seguimiento de posibles objetivos a distancia por SMS o Internet.[6] Este sistema es exclusivo para ubicar los vehículos y objetos. Es preciso indicar que no sólo existen los GPS descritos, sino que hay una amplia gama más desarrollada en otros estados.

c) Funcionalidad

Estos sistemas tienen funciones básicas como la información sobre: *a*) el posicionamiento, *b*) navegación y *c*) cronometría; la primera se refiere al lugar en el cual se ubica una persona u objeto; la navegación se refiere a la ruta de

[5] Docplayer, "Rastreadores GPS tracker".
[6] *Loc. cit.*

desplazamiento de la persona u objeto, y la cronometría se encarga de la medición del tiempo. Estos datos sirven para determinar el lugar, el espacio y el tiempo en el cual se ubica a una persona u objeto; para efecto de nuestro objeto de investigación, solo abordaremos si con este sistema se puede obtener de manera precisa y exacta la localización de la persona que realizó un hecho presuntamente constitutivo de delito.

Dentro de los usos más generales del GPS están la prevención de robos, secuestros, privación ilegal de la libertad, la vigilancia de las personas y los sujetos activos de los hechos delictivos y la vigilancia en los diversos espacios de un Estado, entre otros.

En la era digital, esta tecnología permite obtener datos de localización geográfica en tiempo real de equipos de comunicación móvil, datos fundamentales para combatir delitos como secuestro, delincuencia organizada, extorsiones o amenazas, entre otros.

II. Riesgos tecnológicos con la geolocalización

En este punto abordaremos algunos de los posibles riesgos de la geolocalización, desde una perspectiva tecnológica, los cuales, por lo general, no los perciben gran parte de los juristas, al ser un conocimiento específico.

Estos riesgos se originan por la complejidad de los sistemas, su infraestructura, los distintos niveles de calidad de los materiales de composición y los recursos económicos destinados para los sistemas de seguridad informática por cada Estado y por los particulares que intervienen en la geolocalización.

Las tecnologías informáticas constituyen el "dispositivo" disciplinario por excelencia, el espacio de realización idóneo para la vigilancia y el castigo. Son formas de control descentralizadas y desterritorializadas que se manifiestan fuera de los espacios institucionales estructurados y se instalan en la esfera íntima.[7] El control del sujeto se traduce en una ocupación mediada tecnológicamente de lo íntimo y lo público: "El biopoder es una forma de poder que regula la vida social desde su interior, siguiéndola, interpretándola, absorbiéndola y rearticulándola".[8]

[7] Paola Ricaurte Quijano *et al*., "Sociedades de control: tecnovigilancia de Estado y resistencia civil en México", p. 266.

[8] *Ibid*.

Por otra parte, algunos de los riesgos que se originan con la utilización de los GPS son: *a*) de infraestructura para GPS: *b*) *hardware*, *c*) de redes y d) otras.

a) De infraestructura para GPS. Son aquellas amenazas que pueden afectar los activos (todos aquellos elementos que hacen parte del correcto funcionamiento de los GPS) por diferentes tipos de problemas, estos pueden ser: Las dependencias a servicio técnico externo, y el poner una red cableada expuesta para acceso no autorizado.[9]

b) De *hardware* para GPS. Las amenazas identificadas para este grupo son hardware que afecta los activos por errores, fallas o degradación. Entre las que encontramos: Infección de sistemas por unidades portables sin escaneo, exposición o extravío de equipo, unidades de almacenamiento, etcétera; la pérdida de datos por error *hardware* y la falta de mantenimiento físico (proceso, repuestos e insumos).[10]

c) De redes de GPS. Las amenazas identificadas en este grupo son las que pueden afectar los activos en transmisión de datos, redes inalámbricas, redes alámbricas; Entre ellas se encuentran: Transmisión no cifrada de datos críticos, red inalámbrica expuesta al acceso no autorizado, acceso electrónico no autorizado a sistemas externos y el acceso electrónico no autorizado a sistemas internos.

d) Otros de los riesgos lo encontramos en que "los sistemas de reconocimiento humano son inherentemente probabilísticos (…). Se puede minimizar la posibilidad de error, pero no se puede eliminar".[11] Esto permite deducir que los GPS puedan tener un error nativo del sistema o del dispositivo, no por causa del humano, y los GPS al leer, ya sea para capturar o identificar el dato, no lo perciba adecuadamente y, como consecuencia, la digitalización se altere haciendo que los ceros y unos no concuerden con la plantilla o formen una incorrecta.

Además, se presenta otro riesgo: "(…) La geolocalización basada en IP representa la asignación de una determinada dirección IP de un dispositivo informático conectado a Internet o dispositivo móvil a su ubicación geográfica

[9] Duvan E. Castro y Ángela D. Rojas, *Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica*, p. 35.

[10] *Ibid*., p. 36.

[11] Consejo Nacional de Investigación, *Reconocimiento biométrico: desafíos y oportunidades*, p. 1.

mundial. Geolocalización utiliza asignación de direcciones IP a: país, región o ciudad, latitud/longitud, ISP, nombre de dominio, etcétera".[12] La IP es importante para identificar la ubicación y el rastreo en tiempo real del presunto responsable.

La importancia de la dirección IP:

> (…) es que se permite rastrear esta dirección en el mundo hasta su dueño o al menos al punto de contacto que puede estar dispuesto a proporcionar los detalles restantes. Al igual que con cualquier otra cosa, la cooperación es casi completamente voluntaria y variará si trabaja con diferentes compañías y gobiernos. Siempre tenga en mente que existen muchas formas para que el hacker enmascare su IP verdadera. En el mundo cibernético de hoy en día, es más probable que sea una dirección IP ilegítima que una real. Así que la IP que se muestra en sus registros tal vez sea lo que conocemos como dirección IP lavada (casi imposible de encontrar).[13]

En contra de lo referido, según expertos "la geolocalización del dispositivo puede ser alterada mediante modificadores del GPS".[14] Los que distorsionan las señales para que no pueda existir comunicación con el exterior y, con ello, se pierda el rastro de la persona o móviles.

De acuerdo con los datos tecnológicos de expertos, tenemos que sí podemos encontrar IP lavadas dentro del sistema de comunicación; generalmente se tiene la creencia de que dicha dirección nos dará la ubicación exacta, pero, como hemos analizado, se puede o no obtener la ubicación exacta o aproximada dependiendo de que la IP sea verdadera, pero existe la posibilidad de sea imposible de encontrar tratándose de la IP lavada; por lo que si se utilizan estos elementos materiales, tratándose de una prueba, esta puede ser idónea o no, dependiendo de la IP y de la calidad de la seguridad informática.

De ahí la importancia de conocer tanto los riesgos como los márgenes de error que puedan presentar los GPS, porque depende de la calidad y la inversión de capital con la que cuente cada sector público o privado para invertir en su ciberseguridad.

[12] *Ibid*.
[13] Stuart McClure *et al*., *Hackers. 6 secretos y soluciones de seguridad en redes*, p. 30.
[14] Red de defensa de los derechos digitales, "Recolección de datos".

Por ello, la localización de datos en tiempo real debe tener más técnicas y tecnologías de calidad para evitar que la IP haga difícil la localización de personas o cosas; hace falta establecer de forma específica algunas leyes preventivas para evitar los riesgos por diseño o defecto del *software* de GPS.También es cierto que el aspecto tecnológico requiere de la tecnología más avanzada del mundo para tener más certeza jurídica, seguridad jurídica, nacional e internacional para obtener mayor exactitud en la localización de personas, y esto implica un alto costo[15] para el Estado o bien para los particulares, lo cual representa un obstáculo para la tan anhelada seguridad jurídica nacional que deben garantizar los Estados, los particulares y las grandes empresas tecnológicas.

III. Los sistemas de posicionamiento global como medio de prueba

Para iniciar nuestro análisis jurídico, delimitaremos nuestro objeto de investigación sólo en la pertinencia de la prueba pericial en materia de informática forense, en el área de conocimiento en materia penal a nivel federal, respecto a los GPS, con relación en la eficacia de los GPS para determinar si es posible localizar el lugar exacto e identificar a las personas que realizaron un hecho presuntamente constitutivo de delito; y si se requiere tener tecnología de punta para mayor exactitud en la localización.

Por tales razones, nuestra investigación la dividimos en tres puntos de acuerdo con las fases del procedimiento penal:[16] *a*) la etapa de la investigación, como un dato de prueba, *b*) la etapa intermedia, como medio de prueba, *c*) en el juicio oral penal, como una prueba pericial forense y, por último, *d*) la valoración de la prueba.

15 Por ejemplo, el precio de la propuesta de una licitación para hasta 7,000 sistemas GPS/DPU (unidades de procesamiento de datos), entre otros, realizada por el Gobierno de la Ciudad de México, representa un costo estimado de $185,236,000.00; la propuesta fue presentada por la empresa Pegaso PCS, S.A. de C.V.

16 Código Nacional de Procedimientos Penales, artículo 211.

III.1. La geolocalización como dato de prueba en la cadena de custodia en la fase de investigación

En el actual sistema penal acusatorio, en el artículo 261[17] del Código Nacional de Procedimientos Penales (CNPP), se define el dato de prueba como un medio de convicción que se advierte idóneo y pertinente; este puede establecer razonablemente la existencia de un hecho delictivo y la presunta responsabilidad del imputado.

En la fase de investigación, en la cual se utiliza la técnica de investigación denominada la "cadena de custodia", se recolectan los datos de prueba. Es esta técnica de investigación la base fundamental para determinar si es eficaz o no una prueba pericial en el juicio oral penal debido a que con la probanza debemos demostrar o desacreditar un hecho probablemente delictuoso en el cual se pretende determinar, el lugar exacto del sujeto activo que tenía el celular que realizó el hecho presuntamente delictuoso, la ubicación exacta de las personas secuestradas o la ubicación del bien, por citar algunos ejemplos.

Ahora bien, para iniciar la fase de la investigación respecto de la geolocalización, realizaremos un análisis jurídico del artículo 303 del CNPP, señalando los actos de investigación que se originan en la orden de localización geográfica en tiempo real o la entrega de los datos conservados y, posteriormente, realizaremos una reflexión sobre la técnica de investigación denominada "cadena de custodia" respecto de la geolocalización como un dato y elemento tecnológico.

III.1.1. Análisis del artículo 303 del Código Nacional de Procedimientos Penales

1. Etapas de la investigación para la orden de localización en tiempo real o la entrega de los datos conservados. El art. 303 del CNPP establece que se requiere iniciar una carpeta de investigación cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada;[18] cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones,

[17] *Ibid*., artículo 261.
[18] *Ibid*., artículo 303, párrafo VII.

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.[19]

De lo que se derivan dos supuestos jurídicos:

a) Uno sobre la localización geográfica en tiempo real, por ejemplo, en caso de la privación ilegal de la libertad, se deberá ordenar a los concesionarios localicen en tiempo real los equipos de comunicación móvil asociados a una línea que se encuentren relacionados con los hechos que se investigan. Si bien es cierto que las concesionarios deberán dar la información de las coordenadas geográficas de latitud y longitud en que se encuentra el dispositivo relacionado con los hechos que se investigan, como lo analizamos en el punto abordado sobre los riesgos tecnológicos, puede haber algún riesgo de no ser tan exactas las referidas coordenadas geográficas. Consideramos que por razones de multiplicidad de tecnologías y las obsolescencias de algunas, o bien, por la falta de recursos de los concesionarios de telecomunicaciones no todos pueden contar con sistema de geolocalización actualizados con la tecnología de punta, lo cual dificultará el valor probatorio.

b) Respecto a la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática hasta un tiempo máximo de noventa días en caso de delitos relacionados o cometidos con medios informáticos. La conservación de datos obliga a sólo utilizarlos para el objeto de investigación y por una duración máxima de 90 días. Los datos conservados se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente.

2. 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, que proporcionen a la autoridad investigadora, con la oportunidad y suficiencia necesarias, la información solicitada para el inmediato desahogo de dichos actos de investigación.[20]

[19] *Ibid*., párrafo II.
[20] *Ibid*., párrafo I.

Destacamos que la información resguardada de acuerdo con las leyes de datos personales tanto en posesión de particulares como de sujetos obligados[21] puede estar en poder de sujetos del sector público o del privado.

3. La autoridad competente, el Ministerio Público o el servidor público en quien se delegue la facultad deberán cumplir, de acuerdo con el artículo 16 constitucional,[22] con los requisitos legales que son: fundar y motivar las causas legales de la solicitud además, expondrán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones[23] a través de la cual se operan las líneas, números o aparatos que serán objeto de la medida para que proporcione con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de los actos de investigación.
4. La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad o en audiencia privada con la sola comparecencia del Ministerio Público. Si la resolución se emite o registra por medios diversos al escrito, los puntos resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público.

En esta fase y una vez que tenga la solicitud, el juez de control debe considerar para sus análisis los debates sobre ¿si debe o no ser autorizada el uso de la geolocalización?, así como el debate de derecho a la privacidad y la libertad; también determinará si la solicitud está debidamente fundada y motivada; si entra dentro de los supuestos permitidos o está ante un caso de excepción. La autoridad judicial federal no podrá autorizar la entrega de la información resguardada 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.[24]

[21] Ley Federal de Protección de Datos Personales en Posesión de los Particulares y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[22] Constitución Política de los Estados Unidos Mexicanos, artículo 16.
[23] Código Nacional de Procedimientos Penales, artículo 303, párrafo III.
[24] Constitución Política de los Estados Unidos Mexicanos, artículo 16, párrafo XIII.

Por ello, para la decisión judicial deberá realizarse el test de proporcionalidad[25] en el cual tendrá que analizar: *a*) la necesidad de la medida, *b*) la proporcionalidad, *c*) idoneidad y *d*) finalidad legítima; dependiendo del caso en concreto, el juez deberá justificar su orden. La petición deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad o en audiencia privada con la sola comparecencia del Ministerio Público.

Si la resolución se emite o registra por medios diversos al escrito, los puntos resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público.[26]

Es pertinente destacar que en el supuesto de que el juez de control niegue la orden de la localización geográfica en tiempo real o la entrega de los datos conservados, el Ministerio Público podrá subsanar las deficiencias y solicitar nuevamente la orden o podrá apelar la decisión; dicha apelación será resuelta en un plazo no mayor de 12 horas a partir de que se interponga.

III.1.2. La técnica de investigación de la cadena de custodia en la geolocalización

La cadena de custodia es un sistema de registro y control que tiene la finalidad de garantizar la autenticidad, mismidad, identidad de objetos o muestras. Es la técnica de investigación aplicable en diversos procesos, es decir, no es limitativo para el tema de la seguridad pública, ni para la impartición de justicia, sino que, por el contrario, su origen es más bien de carácter laboratorial y cabe su aplicación en el ámbito de las investigaciones de hechos que sean probables delitos, así como en la secuela de los procesos de impartición de justicia en los que se aporten elementos materiales como medio de convicción, ya sea que se hubieren recolectado en una investigación de campo o bien que hubieran sido aportados por alguna persona a la autoridad competente: "La cadena de custodia servirá como medio para garantizar la legitimidad, identidad, integridad e incluso hasta el debido proceso".[27]

La cadena de custodia se inicia con la preservación del lugar de la intervención por el Primer Respondiente y/o Policía con Capacidades para Proce-

[25] Diana B. González y Rubén Sánchez, *El test de proporcionalidad. Convergencias y divergencias*.
[26] Código Nacional de Procedimientos Penales, artículo 303, párrafo V.
[27] Oscar D. Ornelas Anguiano, "La cadena de custodia en el proceso penal mexicano".

sar, la cual tendrá como principal objetivo la custodia y vigilancia del lugar de intervención con el fin de evitar cualquier acceso indebido que pueda causar la pérdida, destrucción, alteración o contaminación de los indicios o elementos materiales probatorios.[28]

Cuando sea necesaria la protección inmediata de los indicios o elementos materiales probatorios o derivado de la inspección de personas o se descubra algún indicio o elemento material probatorio, se deberá realizar la recolección a efecto de evitar la alteración, destrucción, pérdida o contaminación de estos; por tal motivo, se llevarán a cabo las acciones de control que sean necesarias.[29]

Para la apertura del empaque/embalaje de indicios o elementos materiales probatorios, en todas las etapas del procedimiento se deberá dejar constancia de su actividad y propósito en el apartado de "continuidad y trazabilidad" del Registro de Cadena de Custodia correspondiente, así como abrir el empaque/embalaje por un lado diferente al cual se encuentra sellado; una vez concluida la actividad, deberá volver a sellarse, estableciendo fecha, hora, lugar, nombre y firma, dejando constancia que fue abierto y vuelto a sellar.[30]

En el supuesto que nos ocupa, la cadena de custodia en la geolocalización requiere la conservación inmediata de datos contenidos en redes, sistemas o equipos informáticos; o bien, la información de las coordenadas geográficas de latitud y longitud en que se encuentra el dispositivo relacionado con los hechos que se investigan. En este último supuesto de un dispositivo celular, los concesionarios o prestadores del servicio de telefonía proporcionarán: una sábana de llamadas del móvil que se está ubicando, que contenga los datos de IMEI, teléfono, BTS y *Azimuth*, análisis de *Azimuth*; indicamos que la fiscalía deberá solicitar la portabilidad. Es importante recordar que si se requiere de la intervención de comunicaciones privadas se hará la solicitud correspondiente de la "situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada"; asimismo, "una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada, salvo que por las características del servicio no los tengan a disposición".[31]

28 Conferencia nacional de custodia guardia nacional, *Cadena de custodia. Guía nacional*, p. 18.
29 *Loc. cit.*
30 *Loc. cit.*
31 Julián Rodríguez Saavedra, *Geolocalización de teléfonos celulares a partir de los datos de tráfico: Medio de prueba en sede penal*, p. 118.

Es pertinente indicar que cuando se requiera intervenir comunicaciones privadas se debe pedir una orden de un juez de control federal especializado en materia de intervención de comunicaciones y cateos. En el supuesto de las comunicaciones entre particulares, podrán ser aportadas voluntariamente a la investigación o al proceso penal cuando hayan sido obtenidas directamente por alguno de los participantes en ella. Las comunicaciones aportadas por los particulares deberán estar estrechamente vinculadas con el delito que se investiga, por lo que en ningún caso el juez admitirá comunicaciones que violen el deber de confidencialidad respecto de los sujetos a que se refiere el CNPP, ni la autoridad prestará el apoyo a que se refiere el párrafo anterior cuando se viole dicho deber. No se viola el deber de confidencialidad cuando se cuente con el consentimiento expreso de la persona con quien se guarda dicho deber.[32]

Como lo hemos verificado a través de la información tecnológica, como con criterios relevantes de la Corte, la geolocalización sólo puede acreditar la localización del celular, pero no de la persona, salvo que se utilicen las biometrías en los GPS.

III.2. Los sistemas de posicionamiento global como medio de prueba

La etapa intermedia tiene por objeto el ofrecimiento y admisión de los medios de prueba, así como la depuración de los hechos controversiales que serán materia del juicio, de acuerdo con el artículo 334 del CNPP.[33]

Esta etapa se compondrá de dos fases: una escrita y otra oral. La fase escrita iniciará con el escrito de acusación que formule el Ministerio Público y comprenderá todos los actos previos a la celebración de la audiencia intermedia. La segunda fase dará inicio con la celebración de la audiencia intermedia y culminará con el dictado del auto de apertura a juicio.

El escrito lo deberán presentar el imputado, el Ministerio Público y la víctima; en tanto, el Ministerio Público deberá formular acusación, la cual contendrá el señalamiento de los medios de prueba que pretenda ofrecer, así como la prueba anticipada que se hubiere desahogado en la etapa de investigación.

[32] Código Nacional de Procedimientos Penales, artículo 276.
[33] *Ibid*., artículo 334.

Si el Ministerio Público o, en su caso, la víctima u ofendido ofrecieran como medios de prueba la declaración de peritos, deberán presentar una lista identificándolos con nombre, apellidos, domicilio y modo de localizarlos; señalando, además, los puntos sobre los que versarán los interrogatorios.

El descubrimiento probatorio consiste en la obligación de las partes de darse a conocer, entre ellas, en el proceso, los medios de prueba que pretendan ofrecer en la audiencia de juicio. En el caso del Ministerio Público, el descubrimiento comprende el acceso y copia a todos los registros de la investigación, así como los lugares y objetos relacionados con ella, como medios técnicos que permitan conocer códigos de identificación o etiquetas técnicas del aparato, o bien, su IMSI o IMEI cuando no hubiera sido posible obtener un determinado número de abonado indispensable en el marco de una investigación.[34]

Tratándose de la prueba pericial, se deberá entregar el informe respectivo al momento de descubrir los medios de prueba a cargo de cada una de las partes, salvo que se justifique que aún no se cuenta con ellos, caso en el cual deberá descubrirlos a más tardar tres días antes del inicio de la audiencia intermedia.[35] Se ofrecen los medios de prueba por escrito. Y en la audiencia intermedia, en la cual el juez de control autorizará el acuerdo probatorio, siempre que lo considere justificado por existir antecedentes de la investigación con los que se acredite el hecho. En estos casos, el juez de control indicará en el auto de apertura del juicio los hechos que tendrán por acreditados a los cuales deberá estarse durante la audiencia del juicio oral.[36]

III.3. La geolocalización como prueba pericial y su valoración

En la última fase del juicio oral penal, se desahogan las pruebas ante el juez, en nuestro caso, en concreto la prueba pericial en informática forense. Para el acreditamiento o desacreditamiento de la prueba electrónica "es funcionalmente adecuado integrar al medio de prueba electrónico una pericial y en algunos casos particulares dentro de la pericial se debe realizar un descubri-

[34] Julián Rodríguez Saavedra, *Geolocalización de teléfonos celulares a partir de los datos de tráfico: Medio de prueba en sede penal*, p. 118.
[35] Código Nacional de Procedimientos Penales, artículo 334.
[36] *Ibid*., artículo 345.

miento o levantamiento de evidencia que establecerán las bases del estudio requerido".[37]

El artículo 272 del CNPP señala que en los peritajes durante la investigación, el Ministerio Público o la Policía con conocimiento de este podrá disponer la práctica de los peritajes que sean necesarios para la investigación del hecho. El dictamen escrito no exime al perito del deber de concurrir a declarar en la audiencia de juicio.[38]

III.3.1. Elementos de prueba pericial en informática forense

Dentro de los elementos de la prueba digital o electrónica, tenemos los soportes materiales (tecnológicos) de los cuales deben, para ser aceptados como lícitos, determinar:

a) el origen o la fuente de origen de la prueba,

b) el contenido del soporte, en nuestro caso, tecnológico,

c) relevancia jurídica, y

d) la licitud de la obtención de la prueba.

Con respecto de los elementos de la prueba digital, tenemos la tesis con número de registro 2013524 que indica:

> En consecuencia, para que su aportación a un proceso penal pueda ser eficaz**, la comunicación debe allegarse lícitamente, mediante autorización judicial para su intervención o a través del levantamiento del secreto por uno de sus participantes pues,** de lo contrario, sería una prueba ilícita, por haber sido obtenida mediante violación a derechos fundamentales, con su consecuente nulidad y exclusión valorativa. De igual forma, dada la naturaleza de los medios electrónicos, generalmente intangibles hasta en tanto son reproducidos en una pantalla o impresos, fácilmente susceptibles de manipulación y alteración, ello exige que para **constatar la veracidad de su origen y contenido, en su recolección sea necesaria la existencia de los registros condignos que a guisa de cadena de custodia, satisfagan el principio de mismidad que ésta persigue,**

[37] Iván Díaz González, "La pertinencia de los cuestionarios y los medios de prueba en los documentos electrónicos".

[38] Código Nacional de Procedimientos Penales, artículo 272.

> **o sea, que el contenido que obra en la fuente digital sea el mismo que se aporta al proceso.** Así, de no reunirse los requisitos mínimos enunciados, los indicios que eventualmente se puedan generar, no tendrían eficacia probatoria en el proceso penal, ya sea por la ilicitud de su obtención o por la falta de fiabilidad en ésta.[39]

De la tesis se establecen como requisitos mínimos que el soporte de prueba no haya sido manipulado, ni alterado, que sea verídico el origen y contenido, y en la recolección sea necesaria la existencia de registros condignos, que en la cadena de custodia satisfagan el principio de mismidad que ésta persigue, o sea, que el contenido que obra en la fuente digital sea el mismo que se aporta al proceso.

En ese contexto, las pruebas idóneas para que el quejoso acredite que se le geolocalizó son: 1. La transferencia de dinero realizada vía electrónica, que refleja imágenes en una pantalla, derivada de la orden dada a un equipo, el cual finalmente editará la información que se le suministró, que fuera a su vez reconocida por la institución bancaria ante la cual se realizó, pues la disposición normativa indicada señala que se le debe geolocalizar al momento de que realice la operación no presencial, y 2. La prueba pericial en materia de informática, que con la utilización de las nuevas tecnologías y los medios electrónicos en la integración, conservación, mantenimiento y verificación de la información genere convicción al juzgador de que se obtuvieron las coordenadas geográficas de latitud y longitud en que se encuentra el equipo que le permitió acceder a la red mundial denominada Internet y que pueda robustecer la veracidad de la transferencia electrónica plasmada en papel ante la falta de reconocimiento de la institución bancaria de dicha transacción.[40]

En el supuesto que considera una detención en flagrancia, en la cual se persigue al sujeto activo que cometió el hecho delictivo sin interrupción alguna a través del sistema electrónico de geolocalización satelital, se ha establecido en tesis aislada, registro digital 2017669,[41] que, a pesar de que no se persigue

[39] Suprema Corte de Justicia de la Nación. Tesis aislada 2013524. Resaltado en negritas por los autores.

[40] Suprema Corte de Justicia de la Nación. Tesis [A.]: II.2o.A.5 A (11a.), Semanario judicial de la Federación y su Gaceta, Undécima Época, tomo IV, libro 18, octubre de 2022, p. 3557.

[41] Suprema Corte de Justicia de la Nación. Tesis [A.]: I.1o.P.110 P (10a.), Semanario judicial de la Federación y su Gaceta, Décima Época, tomo III, libro 57, agosto de 2018, p. 2688.

físicamente e inmediatamente, "(...) si la detención del sujeto activo se realizó enseguida de que cometió el hecho delictivo —lapso razonable— en virtud de que se persiguió mediante un sistema electrónico de geolocalización satelital de momento a momento (...)". Se cumplía con lo dispuesto en el artículo 16 párrafo quinto de la Constitución Política de los Estados Unidos Mexicanos en correlación con el abrogado artículo 267 párrafo primero del Código de Procedimientos Penales para el Distrito Federal y, por tanto, no se trató de un acto arbitrario porque la policía justificó la detención en flagrancia, pues cumplió con los elementos exigidos, por ende, no se vulneraron derechos fundamentales.

Por último, es pertinente indicar que los GPS generan riesgos tecnológicos:

> (...) la actualización de los mapas, un 50% de los encuestados ha tenido problemas con ello, y la mala recepción de la señal del satélite, un 43% de los encuestados. Otro 25% ha sufrido inconvenientes para localizar una dirección o localidad, consecuencia del *software* o de los mapas. La visibilidad de la pantalla también ha provocado problemas para un 20% de los usuarios. Algo muy a tener en cuenta por parte de los fabricantes.

Los riesgos que presentan los GPS en algunas ocasiones hacen imposible la localización exacta y sólo se puede obtener una aproximada del dispositivo móvil y no necesariamente del probable responsable de la conducta delictuosa.

Se ha establecido que sólo la geolocalización sirve para ubicar el dispositivo, pero no a las personas que cometieron la conducta ilícita. Ahora, con la tecnología de rastreo, se dice que sí es posible por el teléfono móvil ubicar al sujeto, sobre todo en los celulares en que se utilizan biometrías para desbloquearlos: "Se debe hacer la extracción pericial una cadena de custodia y además se debe demostrar que el celular fue desbloqueado con elementos biométricos con ello la ubicación del celular y del dueño del mismo se pueden vincular de igual forma se puede solicitar a la autoridad competente la información de las sábanas de llamadas, para fortalecer aún más el valor probatorio".[42]

[42] Duriva, "Geolocalización celular como prueba pericial en informática".

III.3.2. Valoración de la prueba pericial informática forense

En el sistema de justicia penal, la prueba pericial informática forense será valorada por los jueces de manera libre y lógica, acatando las reglas de sana crítica observando los conocimientos científicos, las máximas de experiencia y derecho.[43]

En el caso de la geolocalización, se tendrá que valorar la prueba pericial, así como los demás elementos probatorios, es decir, los elementos materiales tecnológicos; primero, respecto al cumplimiento de la legalidad, para tener acceso a las comunicaciones privadas; también, que no se hayan vulnerados derechos fundamentales, como el derecho a la libertad y la privacidad, que se haya cumplido con el deber de confidencialidad para efecto de que no esté afectadas de ilicitud y de nulidad. Posteriormente, se deberá valorar cada medio tecnológico que integra el sistema de posicionamiento geográfico respecto a su integridad, contenido y conservación; además, deberán cumplir el principio de mismidad, todo de manera integral, lo cual puede ser difícil de valorar dada la multiplicidad de tecnologías y de riesgos tecnológicos, los cuales deberán ser objetos de investigaciones posteriores.

IV. Conclusiones

La geolocalización, dependiendo de la calidad e idoneidad de su sistema, será más o menos exacta en la precisión del lugar debido a que existe una multiplicidad de tecnologías que pueden ser de punta u obsoletas, lo cual conlleva a la falta de certeza jurídica porque no garantizan la seguridad jurídica e informática, y puede ser que no tengan valor probatorio en una prueba pericial de informática forense.

La evolución de los GPS muestra que cada vez son más exactos, lo cual repercute en que sean más confiables y adquieran mayor certeza jurídica, sobre todo cuando se utilizan en los celulares desbloqueados con biometrías o sistema de autentificación biométricos. Sin lugar a duda, se tiene que analizar cada caso en particular para poder ver la idoneidad de la prueba pericial en el caso de la geolocalización, pues dependerá de qué tan obsoleta es la tecnología o de qué tan actualizada para poder determinar si es posible o no ubicar a las personas.

[43] Alberto E. Nava Garcés, *La prueba electrónica en materia penal*, pp. 215-216.

Fuentes de consulta

Bibliográficas

McClure, Stuart, Joel Scambray y Kurtz George. *Hackers. 6 secretos y soluciones de seguridad en redes*. (Trad.), Jorge Arturo Pineda Sánchez, México, McGraw-Hill, 2010.

Nava Garcés, Alberto Enrique. *La prueba electrónica en materia penal*. México, Porrúa, 2015.

Electrónicas

Castro Bolaños, Duvan Ernesto y Ángela Dayana Rojas Mora. *Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica*. Trabajo de grado para optar al título de Ingeniero de Sistemas, Universidad Católica de Colombia, 2013. https://core.ac.uk/download/ 71892900.pdf

Conferencia Nacional de Custodia Guardia Nacional. *Cadena de custodia. Guía nacional*. https://www.criminalistasforenses.org.mx/docs/cadena-de-custodia_guia-nacional.pdf (consultada el 8 de enero de 2023).

Consejo Nacional de Investigación. *Reconocimiento biométrico: desafíos y oportunidades*. Washington, 2010. http://www.nap.edu/openbook.php?record_id= 12720&page=1 (consultado el 24 de julio de 2022).

Díaz González, Iván. "La pertinencia de los cuestionarios y los medios de prueba en los documentos electrónicos". *Abogado Digital,* 10 de noviembre de 2022. https://www.abogado.digital/la-pertinencia-de-los-cuestionarios-y-los-medios-de-prueba-en-los-documentos-electronicos/ (consultado el 10 de enero de 2023).

Docplayer. "Rastreadores GPS tracker". https://docplayer.es/47853663-Rastreadores-gps-tracker.html (consultado el 3 de febrero de 2023).

Duriva. "Geolocalización celular como prueba pericial en informática". https://duriva.com/geolocalizacion-celular-como-prueba-pericial-en-informatica/ (consultado el 10 de enero de 2023).

Miip.org. Geolocalización IP y dominios. http://miip.org/localizar-ip.php (consultada el 7 de enero de 2023).

Gps.gov. "El sistema de posicionamiento Global". Oficina de coordinación nacional de posicionamiento, navegación y cronometría por satélite. https://www.gps.gov/systems/gps/spanish.php (consultada el 7 de febrero de 2023).

González Carvallo, Diana Beatriz y Rubén Sánchez Gil (coords.). *El test de proporcionalidad. Convergencias y divergencias*. México, Suprema Corte de Justicia de la Nación. 2021. https://www.sitios.scjn. gob.mx/cec/sites/default/files/publication/documents/2022-02/05_La%20 finalidad%20legi%CC%81tima%20en%20el%20test%20de%20proporcionalidad%20y%20en%20la%20Suprema%20Corte%20de%20Justicia%20de%20la%20Nacio%CC%81n.pdf

Instituto Federal de Telecomunicaciones. "Glosario". http://www.ift.org.mx/que-es-el-ift/glosario (consultada el 16 de abril 2023).

Organización de las Naciones Unidas. *Declaración Universal de Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights. (consultada el 14 de enero de 2023).

Ornelas Anguiano, Oscar Daniel. "La cadena de custodia en el proceso penal mexicano. Estudios Forenses". *Revista Electrónica del Instituto Jalisciense de Ciencias Forenses,* año 1, núm. 1, marzo-septiembre 2020. http://www. estudiosforenses.mx/articulo.php?id=8#:~:text=La%20cadena%20de%20custodia%20es%20el%20sistema%20de%20control%20y,autoridad%20competente%20ordene%20su%20conclusi%C3%B3n.

Red de defensa de los derechos digitales. "Recolección de datos". 23 de marzo de 2021. https://r3d.mx/2021/03/23/recoleccion-de-datos-de-geolocalizacion-en-banca-en-linea-es-desproporcionada-riesgosa-e-innecesaria/ (consultado el 13 de enero de 2023).

Ricaurte Quijano, Paola, Jacobo Nájera y Jesús Robles Maloof. "Sociedades de control: tecnovigilancia de Estado y resistencia civil en México". *Teknokultura revista de cultura digital y movimientos sociales,* 11, (2), pp. 259-282. https://revistas.ucm.es/index.php/TEKN/article/viewFile/48241/45136 (consultado el 13 de enero de 2023).

Rodríguez Saavedra, Julián. *Geolocalización de teléfonos celulares a partir de los datos de tráfico*: *Medio de prueba en sede penal*. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile. https://repositorio.uchile.cl/bitstream/handle/2250/184555/Geolocalizacion-de-telefonos-celulares-a-partir-de-los-datos-de-trafico-medio-de-prueba.pdf?sequence=1

Legislación

Código Nacional De Procedimientos Penales, publicado en el *Diario Oficial de la Federación* el 5 de marzo de 2014; última reforma publicada el 19 de febrero de 2021.

Constitución Política de los Estados Unidos Mexicanos, publicada el 5 de febrero de 1917 en el *Diario Oficial de la Federación*; última reforma publicada en el 8 de mayo de 2023.

Diario oficial de la Unión Europea. Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009. https://edps.europa.eu/sites/edp/files/publication/dir_2009_136_es.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada el 5 de julio de 2010 en el *Diario Oficial de la Federación*.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017 en el *Diario Oficial de la Federación.*

Ley Federal de Telecomunicaciones y Radiodifusión, publicada en el *Diario Oficial de la Federación* el 14 de julio de 2014; última reforma publicada en el 20 de mayo de 2021.

Suprema Corte de Justicia de la Nación. Crónicas del pleno y de las salas. Primera sala: es constitucional la localización geográfica de los equipos de comunicación móvil, cuando se está frente a la búsqueda de víctimas. https://www.scjn.gob.mx/

sites/default/files/sinopsis_asuntos_ destacados/documento/2017-02/1S-180516-AZ-LL-3886.pdf

Suprema Corte de Justicia de la Nación. Tesis aislada 2025357. Gaceta del Semanario Judicial de la Federación. Libro 18, octubre de 2022, Tomo IV, página 3557. https://sjf2.scjn.gob.mx/detalle/tesis/2025357 (consultada el 08 de febrero de 2023).

Suprema Corte de Justicia de la Nación. Tesis aislada 2013524. Gaceta del Semanario Judicial de la Federación. Libro 38, enero de 2017, Tomo IV, página 2609. https://sjf2.scjn.gob.mx/detalle/tesis/ 2013524 (consultada el 08 de febrero de 2023).

Suprema Corte de Justicia de la Nación. Tesis aislada 2017669. Gaceta del Semanario Judicial de la Federación. Libro 57, agosto de 2018, Tomo III, página 2688. https://sjf2.scjn.gob.mx/detalle/tesis/ 2017669 (consultada el 08 de febrero de 2023).