IUS ET SCIENTIA
2022 • Vol. 8 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2022

El entrecruce entre la tecnología y los medios probatorios. El caso de la intervención de comunicaciones en México

THE INTERSECTION BETWEEN TECHNOLOGY AND EVIDENCE. COMMUNICATIONS INTERCEPTION IN MEXICO

Paola de la Rosa Rodríguez
Universidad Autónoma de San Luis Potosí
paola.delarosa@uaslp.mx 0000-0001-6620-3589

Recibido: 09 de junio de 2022 | Aceptado: 24 de junio de 2022

RESUMEN

En la actualidad han emergido nuevas formas de comprobar conductas ilícitas realizadas con y a través de las tecnologías. Este artículo analiza el carácter instrumental que tiene la tecnología como coadyuvante del derecho en la procuración y administración de la justicia penal. Específicamente, su papel en la obtención de medios de prueba dentro de un proceso judicial que tiene como objetivo la búsqueda de la verdad. El trabajo consta de dos partes. En la primera se explora la importancia del empleo de instrumentos tecnológicos y herramientas digitales para investigar las formas de comisión de conductas ilícitas. Se explica la prueba electrónica, su obtención, incorporación y ofrecimiento dentro de un proceso penal. En la segunda parte y ante el creciente uso de los medios tecnológicos en la investigación criminal, se estudia el caso de la intervención de comunicaciones y la afectación que ésta tiene en los derechos fundamentales en México.

PALABRAS CLAVE

Dispositivos electrónicos
Evidencia digital
Intervención de comunicaciones
Prueba electrónica
Tecnología y medios probatorios

ABSTRACT

In today's world, new ways of verifying ilegal conduct carried out with and through the use of technologies have emerged. This article analyzes the instrumental nature of tecnhology as a support for the law in the prosecution and prosecution of criminality. Specifically, its role in obtaining pieces of evidence within a judicial process and the search for truth. The paper consists of two parts. The first explores the importance of using technological instruments and digital tools to investigate forms of illicit conduct. It explains electronic evidence, ways of obtaining, offering and incorporating it into Court. Having in mind the increasing use of technological means in criminal investigation, the second part explains communications interception and the impact it has on fundamental rights in Mexico.

KEYWORDS

Electronic devices
Digital evidence
Communications interception
Electronic evidence
Technology and evidence

I. Introducción

En una época en donde dependemos de la tecnología para realizar nuestras actividades y en donde las plataformas digitales se han integrado a nuestro quehacer diario, los avances tecnológicos también han permeado en la implementación de la justicia. La tecnología ha modificado las prácticas del derecho, originando que cada vez sea más común que los profesionales del litigio se enfrenten a resolver controversias en donde resultan involucrados aspectos tecnológicos que rebasan el conocimiento común y el ámbito de la experticia común.

Núñez Jover (2007) y Lucas (2014) afirman que al hablar de la sociedad contemporánea es ineludible hablar de la tecnología moderna. A manera de ejemplo, la revolución tecnológica ha permeado en el área de la comunicación pasando desde el telégrafo, al teléfono hasta el día de hoy con la innovación de los smartphones; en el ámbito de la salud existen ahora diversos conocimientos y maquinaria para investigar y curar enfermedades, mientras el ámbito educativo y laboral se ve beneficiado por las reuniones, plataformas y herramientas digitales (Yañez, 2015). Jijena, Palazzi y Tellez (2003) han referido que somos parte de sociedades cada vez más interconectadas e interdependientes.

Asi también, los avances de la era tecnológica han hecho posible nuevas conductas y formas de proceder, unas están permitidas por la ley, sin embargo otras se encuentran prohibidas y son castigadas por la norma. En este contexto y ante el surgimiento de comportamientos llevados a cabo a través de instrumentos tecnológicos, los procedimientos judiciales resienten asimismo estos cambios. En otras palabras, el derecho se está adaptando a las nuevas conductas que son llevadas a cabo en la sociedad a través de medios digitales.

En este orden de ideas, siguiendo a Cossío (2017), la evolución de la ciencia y la tecnología exige regular las nuevas actividades con el fin de dotarlas de orden y permitir la solución de controversias. Joan Pico (2017) señala que la prueba de expertos es fundamental para la justa resolución del proceso en aquellos casos en los que el juez precisa de conocimientos científicos, técnicos o especializados. Dicha situación puede observarse más fácilmente en el uso de conocimiento especializado para la comprobación de hechos dentro de un procedimiento. En específico, los medios utilizados para acreditar los hechos en un proceso judicial también han evolucionado originando la denominada: prueba electrónica.

Las sociedades actuales se caracterizan por el uso ordinario de tecnologías provenientes de conocimientos cada vez con mayor grado de especialización y de muy diversos tipos. El conocimiento tecnológico ha evolucionado también el mundo jurídico, no únicamente en la aplicación de nociones técnicas sino en el enorme auge de la utilización de este recurso, en la resolución de casos penales.

En el entorno criminal, hoy en día se cometen crímenes a través de las diversas páginas, aplicaciones y redes que son accesibles a través de internet. En forma preocupante, la capacidad que ahora tiene una sola persona de dañar o afectar a un gran número de individuos está aumentando exponencialmente, debido al uso de la red. En este sentido, internet permite cometer más delitos y permite actuar a mayor escala. Dicho sea

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

de paso, los delincuentes están empleando la tecnología para facilitar la ejecución de conductas ilícitas en forma inmediata, a gran escala y en varios puntos del planeta pudiendo ahora observarse un notable incremento en la cantidad de recursos y documentos electrónicos en la comisión de los delitos así como un rápido aumento de piratas informáticos que hacen uso de soportes electrónicos y desarrollan sus delitos a través de internet. Esto es, mientras más avances se conocen en el área de la computación, más y mejores medios y métodos son utilizados para delinquir.

En razón a lo anterior, los internautas tenemos que optar por la adopción de mecanismos de seguridad pues de otra forma nuestra información se ve comprometida. Derechos tales como la propiedad, privacidad e integridad se ven transgredidos por otros usuarios de la red.

Es ampliamente conocido que han emergido formas de comunicación a través de correo electrónico y más recientemente mediante el empleo de redes sociales; pues bien, esta información resulta útil dentro de un procedimiento penal. Es así que las partes en un juicio recurren a medios probatorios derivados del uso de dispositivos digitales. De hecho, cada vez es más recurrente que las partes acrediten sus pretensiones a través de la comunicación sostenida a través de correos electrónicos, mensajes instantáneos de WhatsApp o redes sociales.

Es difícil delimitar los tipos de prueba electrónica debido a las numerosas innovaciones tecnológicas y científicas. El correo electrónico y a los mensajes derivados de aplicaciones de mensajería instantánea son medios a través de los cuales se puede comprobar la ocurrencia de un determinado hecho con apariencia de delito.

El correo electrónico que consiste en intercambio de textos digitalizados como imágenes, vídeos o audios, hace posible la emisión instantánea de mensajes a un receptor a través de una dirección electrónica (López, 2006). Todo correo electrónico podrá constituir una prueba electrónica siempre que se cubran los requisitos para su correcta obtención e incorporación.

WhatsApp es un sistema de mensajería para telefonía móvil que permite el intercambio de mensajes ilimitados, así como de imágenes, vídeos, notas de audio, contactos e incluso la ubicación en tiempo real entre los contactos que de alta el teléfono del usuario (Vaqueira, 2014).

Haciendo referencia a las pruebas, de acuerdo a Parra (2006) éstas son la columna vertebral de un proceso judicial pues con ellas se demuestran los hechos materia del litigio. Incluso se ha dicho; "sin la prueba en el proceso, la arbitrariedad seria la que reinaría." La prueba es el puente entre el derecho procesal y el sustancial, de tal manera que las diversas garantías procesales y probatorias son instrumentos de validez constitucional de la decisión del juez sobre la verdad jurídica y la verdad fáctica (Ruiz Jaramillo, 2007).

Hoy en día los avances científicos y tecnológicos tienen gran relevancia para apoyar en los métodos de búsqueda de la verdad. Tal es el caso que el descubrimiento de nuevas técnicas y metodologías de investigación en diversos campos del conocimiento amplían progresivamente el ámbito de lo que puede ser corroborado científicamente. Si bien anteriormente la comprobación de los hechos se dejaba al sentido común

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

y a pruebas tradicionales, hoy en día se aplican métodos científicos y tecnológicos para corroborar un hecho. En atención a lo anterior, podemos hacer referencia a que nos encontramos ante diligencias de investigación novedosas que presentan ciertas particularidades.

Incorporar la tecnología como coadyuvante para la procuración de justicia plantea muy diversos problemas que han sentado intensas discusiones entre los académicos y operadores del sistema de justicia. Por ejemplo, la obtención de este tipo de pruebas requiere la intervención de expertos que conozcan de evidencia electrónica, puesto que tanto la obtención como el procesamiento tanto del dispositivo en que se encuentra la información así como de los datos mismos que conforman la prueba necesitan cubrir protocolos especificos. Además, muchas veces pueden resultar muy intrusivas en la esfera de los derechos fundamentales de los individuos sujetos a una investigación criminal, resultando imprescindible contar con una normativa con enfoque de derechos humanos y adaptada a la nueva realidad tecnológica. Estos entornos ameritan el surgimiento de un moderno Derecho probatorio que permita acreditar los hechos y demostrar nuevas posibilidades de actuación. Ante esta diversificación y transformación de la delincuencia, que tiende a ser lucrativa, el Estado debe de asumir una forma diferente de tratar la ciberdcelincuencia.

II. La prueba electrónica

¿Cuál es el medio para convencer al juez sobre la existencia y modalidades de los hechos, es decir cómo se prueba la comisión de una conducta ilícita cometida en el terreno cibernético?

Como sabemos, cada actividad que lleva a cabo el ser humano va dejando huellas y rastros en su andar. No obstante, Marc Goodman (2003), con estudios en Medicina Forense Computarizada y en la investigación de delitos vía internet, quien estuvo encargado de la Unidad de Internet del Departamento de Policía de los Ángeles señala que el mundo digital no deja huellas de sangre y por lo que es más difícil perseguir lo que ha ocurrido." Siguiendo a este autor, el Departamento de Defensa de los Estados Unidos llevó a cabo miles de intromisiones intencionales en las computadoras del Gobierno Federal, de las cuales noventa y nueve por ciento no fueron detectadas por los sistemas del ejército; tampoco se identificaron a los hackers ni los ataques. Entonces, ¿cuáles son los recursos con los que se cuentan para perseguir y atacar el problema?

Como premisa, Arazi (2008) refiere que si los medios de comisión de un delito fueron electrónicos, por lo general existirán constancias como por ejemplo los discos duros de las computadoras los cuales son fuente importante para acreditar hechos. Luego entonces, las mismas tecnologías pueden convertirse en herramientas que auxilian la justicia y la persecución de delito y el delincuente. Es así que derivado de la propagación de delitos informáticos y la necesidad de combatirlos y no dejarlos impunes, es necesario entender los particulares medios con los que se cometió un ilícito así como la forma de demostrar su intervención para eventualmente identificar al autor o autores del crimen.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

Una de las controversias que surgen de la persecución de este tipo de delitos es que estos medios con los que se puede probar la comisión de un ilícito suelen ser complejos en su análisis, así por ejemplo la cantidad de información que puede almacenar una computadora personal es considerable tanto como lo es el contenido de un disco duro de diez Gb. Debido a la cantidad de información que puede almacenar, es muy distinto catear y registrar una casa a obtener la información de un disco duro de diez Gb.

Por otra parte, los ciberatacantes se toman ventaja del anonimato de utilizar internet pues por ejemplo, se pueden enviar correos electrónicos sin los datos del emisor utilizando un servidor que borra la información del emisor original, y se puede cambiar la dirección de correo electrónico. Es ampliamente conocido que no hay forma de comprobar que la información que ingresamos para dar de alta una cuenta de correo sea verídica. No obstante, existen recursos para demostrar una actividad realizada mediante dispositivos electrónicos. En estos contextos surge la prueba electrónica la cual se expresa mediante un soporte electrónico, creado por los modernos instrumentos tecnológicos de información.

La prueba electrónica o prueba digital ha sido definida como toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio (Delgado, 2017). De esta definición se desprende que es cualquier información que ha de ser producida, almacenada o transmitida por medios electrónicos, que pueda tener efectos para acreditar hechos en el proceso. Incluye no únicamente archivos sino también logs y otra información no generada directamente por la persona. Por su parte, Arazi (2008) hace referencia al concepto de Colerio para quien la prueba electrónica en sentido amplio está asentada en un registro cuyo soporte no es papel y en su información, archivo o registro interviene un medio electrónico, entendido este término no en un sentido técnico-científico, sino vulgar y abarcativo de todo supuesto de desmaterialización electrónica de la declaración que tradicionalmente se vuelca y conserva en el tradicional soporte papel. Este tipo de prueba aporta una cantidad ilimitada de nuevos medios probatorios, algunos aún sin conocer, por los avances en la ciencia y tecnología.

La prueba electrónica demanda complejidad para su obtención debido a su componente técnico-científico, lo que exige pruebas o pericias informáticas así como criterios valorativos clave. Este tipo de prueba no representa una superioridad probatoria pero requiere del apoyo de otras pruebas para un ejercicio de valoración. A continuación se señalan los momentos o etapas de la prueba electrónica dentro de un proceso judicial.

III. Momentos de la prueba electrónica

1. Obtención de la información o datos: obtención de los datos o información
2. Incorporación
3. Ofrecimiento
4. Valoración

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

IV. Obtención de la prueba electrónica

La primera etapa o momento se refiere a la obtención de los datos o información producida, almacenada o transmitida mediante el acceso a las fuentes de la prueba electrónica o digital, antes de su incorporación al proceso. Más específicamente, es acceder a la información o datos producidos o almacenados en un dispositivo electrónico, o bien transmitidos en forma electrónica a través de redes de comunicación abiertas o restringidas como internet, telefonía fija, móvil u otras.

La importancia de esta etapa radica en que el abogado litigante necesita conocer si se siguieron las formalidades en la recolección de este tipo de evidencia debido a que la obtención que no haya seguido los procedimientos apropiados será ilegal o irregular y en algunos casos, habiéndose afectado derechos fundamentales de las personas indiciadas, se tratará de una prueba ilícita (De la Rosa, 2019).

V. Cateo y aseguramiento de la prueba electrónica

En primer término señalamos que el cateo es una diligencia prevista en el texto constitucional el cual tiene como objetivo buscar objetos o personas para acreditar un delito.

Para la práctica del cateo de bienes informáticos debe de existir una orden judicial expresa en la que se mencione:

— El lugar que ha de inspeccionarse,
— La persona o personas que hayan de aprehenderse y
— Los objetos que se buscan

La cadena de custodia comienza desde que se identifica un indicio y termina cuando la autoridad solicitante así lo dispone. Es necesario que un agente del Ministerio Público de fe del estado físico en que se encuentra la computadora y el disco duro, la documentación de la cadena dará certeza de que esto ocurrió

La cadena de custodia se debe de llevar a cabo conforme a los procedimientos establecidos en los protocolos para que exista certeza de que no fue objeto de manipulación. Debe por lo tanto existir un ordenamiento que establezca el protocolo tratándose de evidencia digital. Si no se siguen puntualmente estos lineamientos, se romperá la cadena de custodia. La ruptura de la cadena de custodia es la interrupción de la secuencia lógica de los procesos que la conforman, la cual puede o no representar una alteración de la evidencia. Se traduce por tanto en la falta de credibilidad del juzgador para determinar si el objeto presentado en la audiencia proviene o es propiedad del sujeto procesado.

VI. Incorporación de la prueba electrónica

La segunda etapa es la incorporación al proceso de la información obtenida la cual deberá ser relevante para la acreditación de los hechos materia de la controversia. Para su

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

incorporación, se debe de tomar en cuenta la pertinencia o relevancia del medio probatorio que acredite los hechos, la licitud con la que se obtuvo o desahogó la información e incluso la utilidad para esclarecer los hechos controvertidos.

Cada caso tiene sus particularidades, no obstante la incorporación se puede realizar por medio de un soporte de papel o bien a través de la aportación de un documento electrónico, que muestre datos contenidos en un soporte electrónico.

Además, hay que tomar en consideración que dependerá de cada evento pero para sustentar una acusación, habrá que ofrecer y desahogar un acervo probatorio en el que la prueba digital sea parte del mismo pero que será complementado con otros medios como testigos, entre otros.

VII. Ofrecimiento de la prueba digital

Se deberá ofrecer en el testimonio del perito cibernético se llevará a cabo en la audiencia intermedia. Solo podrá ofrecerse si se acreditan, en principio, su ilicitud y que en el proceso de obtención se ha respetado la cadena de custodia. El oferente deberá aclarar su pretensión probatoria, el alcance de la misma, la legalidad del caudal ofrecido y el haber cumplido y cubierto los requisitos de la cadena de custodia.

VIII. Valoración de la prueba electrónica

El juez debe adecuarse a las innovaciones tecnológicas, respetando las garantías constitucionales del debido proceso. Si bien es cierto se requiere de conocimientos informáticos por parte de jueces, se hace necesario de peritos informáticos o peritos en cibernética para que expliquen la necesidad de la injerencia realizada en el equipo, la autorización para proceder a ello, el procedimientos y los recursos empleados en el mismo, e incluso aclaren terminología empleada. La prueba pericial debe de explicar lo sucedido y ofrecer conclusiones claras y científicamente avaladas.

La tercera fase, que consiste en la valoración de la información por el juez, tendrá lugar una vez desahogadas las pruebas, en la audiencia de juicio oral. Dicha evaluación probatoria dependerá del interrogatorio que de viva voz se haga al perito en informática para verificar si se cumplieron los requisitos para la obtención y práctica.

IX. La investigación de dispositivos electrónicos. El caso de la intervención de las comunicaciones por medios electrónicos

Como antecedente, la inviolabilidad de las comunicaciones en México se estableció en la reforma constitucional de 1996, dando origen a que la regulación sobre la intervención de comunicaciones estableciera las modalidades o formas para que una intervención sea lícita.

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

Es necesario señalar que la intervención o interceptación de las telecomunicaciones se realiza través de la colocación de un sistema *packet sniffer* (rastreador de paquetes). Este rastreador es un programa que se coloca en un espacio por el que circulan flujos de datos. Mencionado lugar puede incluso ser alguna de las miles de redes por las que frecuentemente fluye información en internet y que aprecian el contenido de los paquetes que transitan en busca de determinados datos, tal es el caso de las contraseñas. Si los paquetes no se envían encriptados, como ocurre frecuentemente, el rastreador leerá y copiará los datos que figuran en ellos.

Cremades *et al* (2009) explican el funcionamiento técnico de la comunicación a través del internet señalando este tema diciendo que "si la red A se comunica con la red B, dicha comunicación no se produce de forma directa entre A y B sino que pasa por cientos o miles de sistemas y redes que forman parte de la internet. Esto explica que dicha comunicación o transferencia de datos se realice por medio de paquetes con direcciones de protocolo de internet (IP). En razón de que la comunicación se lleva a cabo por medio de paquetes que circulan por un gran número de sistemas y redes intermedios, puede suceder que la comunicación llegue deteriorada o con errores. Los autores refieren que al dividir la transmisión de datos total en millones de pequeños paquetes, si alguno de ellos arriba con distorsiones al sistema de destino, únicamente es necesario que el sistema o red que lo ha remitido nuevamente envíe ese paquete dañado, no la totalidad de los datos objeto de la transmisión.

Cuando se quebrantan la totalidad de los datos transmitidos en millones de paquetes es preciso, poder identificar al sistema que expide dichos paquetes. Esto se consigue mediante las direcciones IP.

Es así que el espionaje informático se configura cuando los datos captados con el *rastreador de paquetes* tengan el carácter de reservados. Esto sucede con los secretos de empresa, o información de gobierno, por mencionar algunos. Las contraseñas que permiten el acceso a un sistema informático, siempre serán privadas y se consideran secreto de empresa. Esta acción constituye un delito cuando se actúa con la intención de descubrir un secreto de empresa.

Hoy en día se establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.[1]

La Constitución Federal Mexicana establece:

> Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.[2]

1. Artículo 6 inciso A, subíndice II de la Constitución Política de los Estados Unidos Mexicanos
2. Primer párrafo del artículo 16 de II de la Constitución Política de los Estados Unidos Mexicanos reformado publicado en el DOF el 15 de septiembre del 2017

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

Por cuanto a la protección de sus datos dispone:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.[3]

Añade que:

> Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.[4]

La inviolabilidad de las comunicaciones forma parte del derecho humano a la privacidad. El Pacto Internacional de Derechos Civiles y Políticos lo consagra en el artículo 17, la Declaración Universal de los Derechos Humanos en el artículo 12, la Convención Americana sobre derechos Humanos en el artículo 11.2. Tal como fue señalado en el cuadro "*Derechos derivados del empleo de medios electrónicos en los tratados internacionales*" del Capítulo Dos.

No obstante, en ciertos delitos de gran impacto social, tal es el caso de la delincuencia organizada, sí se podrán intervenir las comunicaciones.

La Constitución Federal establece que, previa petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, la autoridad judicial federal podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud y expresar el tipo de intervención, los sujetos de la misma así como su duración.[5]

Es así que la intervención de comunicaciones se contempla en el Capítulo Primero del Título Segundo de la Ley Federal contra la Delincuencia Organizada que establece las reglas generales para la investigación de este tipo de criminalidad:

> Cuando en la investigación el Ministerio Público de la Federación considere necesaria la intervención de comunicaciones privadas el Titular de la Procuraduría General de la República o los servidores públicos en quienes se delegue la facultad podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.[6]

3. Segundo p*árrafo del artículo 16 de* II de la Constitución Política de los Estados Unidos Mexicanos reformado publicado en el DOF el 15 de septiembre del 2017
4. Párrafo doce del artículo 16 de II de la Constitución Política de los Estados Unidos Mexicanos reformado publicado en el DOF el 15 de septiembre del 2017
5. Párrafo trece del artículo 16 de la Constitución Política de los Estados Unidos
6. Artículo 16 de la Ley Federal de delincuencia Organizada publicada en el Diario Oficial de la

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

Mencionada ley añade que la solicitud deberá ser resuelta por la autoridad judicial en forma inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público de la Federación, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público de la Federación.[7]

El Código Nacional de Procedimientos Penales dispone:

> La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.[8]

También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos.[9]

De acuerdo a la Ley Orgánica del Poder Judicial de la Federación, es el juez de control quien debe de otorgar la autorización de intervención de comunicaciones privadas, previa solicitud del Ministerio Público de las entidades federativas. Deberá de darse respuesta judicial de forma inmediata, por cualquier medio que no ponga en duda su autenticidad.[10]

La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención.[11]

Federación el 7 de noviembre de 1996, Última reforma publicada DOF el 7 de abril del 2017.

7. Artículo 17 de la Ley Federal de delincuencia Organizada publicada en el Diario Oficial de la Federación el 7 de noviembre de 1996, Última reforma publicada DOF el 7 de abril del 2017.
8. Artículo 292 del CNPP Párrafo reformado y publicado en el DOF el 17 de junio del 2016
9. Párrafo adicionado DOF 17-06-2016
10. 50 bis y 50 Ter de la Ley Orgánica del Poder Judicial de la Federación
11. Artículo 292 CNPP

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

X. Centro especializado en técnicas de investigación y Juez de arraigos, cateos e intervención de comunicaciones

El creciente número de prácticas de investigación en casos de delincuencia organizada, da origen al Centro Nacional de Justicia Especializado en el control de técnicas de Investigación, arraigo e intervención de comunicaciones (CNJECTIAIC) el cual surge a partir del Acuerdo General 3/2017 del Pleno del Consejo de la Judicatura Federal reportando una carga de trabajo de 2880 eventos entre el 6 de julio de 2018 al 28 de mayo del año 2019. Por otra parte, de acuerdo al Censo Nacional de Impartición de Justicia INEGI (2018) en México, la creación de esta figura se deriva del acuerdo 20/2018 del Pleno del Consejo de la Judicatura Federal, relativo a la conclusión de funciones de los Juzgados Primero y Segundo Federales Penales Especializados en Cateos, Arraigos e Intervención de Comunicaciones. Tienen competencia en toda la República y residencia en la Ciudad de México. Entraron en funciones el 15 de agosto del mismo año.

Estos cambios obedecen a la reforma en los ordenamientos contra la delincuencia organizada en México. Los cambios generados en el año 2016 se perciben restrictivos de derechos humanos ya que la Procuraduría, ahora Fiscalía General de la República puede intervenir comunicaciones privadas en menos de seis horas no siendo necesario que demostrar ante el juez indicios de que la persona intervenida o espiada tiene nexos con el crimen organizado. Antes de las reformas, el juez tenía un plazo de doce horas para autorizar la intervención de comunicaciones de un individuo. Además, se pueden realizar espionajes en tiempo real en sitios públicos por cualquier medio tecnológico o electrónico y llevar a cabo operaciones con agentes encubiertos. La intervención, sin embargo, no podrá exceder de seis meses.

Si bien son modificaciones que tienen por propósito combatir el crimen organizado, los defensores de derechos humanos sostienen que la violación de comunicaciones privadas se actualiza en el momento en que se escucha, graba, almacena, lee o registra una comunicación sin autorización de sus interlocutores. Si bien no es necesario para intervenir comunicaciones demostrar ante un órgano judicial que una persona tiene vínculos con la delincuencia organizada, al intervenirla se disuelve la intimidad de una persona, queda expuesta, debilitada ante la mirada o escucha arbitraria, restándole autonomía y dejando su privacidad a merced del Estado.

XI. Criterios jurisprudenciales en torno a la inviolabilidad de las comunicaciones en México

Valga en esta parte hacer una relación de las tesis de la Suprema Corte de Justicia de la Nación:

Este primer criterio establece que no obstante la Constitución Federal prevé la intervención de comunicaciones, las injerencias estatales en conversaciones entre particulares no se podrán utilizar si no fueron autorizadas por un funcionario judicial. Aquí el criterio:

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

FACULTAD DE INVESTIGACIÓN PREVISTA EN EL ARTÍCULO 97, PÁRRAFO SEGUNDO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. LA IMPOSIBILIDAD CONSTITUCIONAL DE OTORGAR VALOR PROBATORIO A LAS GRABACIONES DERIVADAS DE LAS INTERVENCIONES DE COMUNICACIONES PRIVADAS OBTENIDAS SIN AUTORIZACIÓN JUDICIAL ES APLICABLE PARA LA VALORACIÓN DE LAS PRUEBAS RECABADAS EN EJERCICIO DE ESA ATRIBUCIÓN. En virtud de que atendiendo a lo previsto en los párrafos noveno y décimo del artículo 16 constitucional las grabaciones obtenidas mediante la intervención de comunicaciones privadas sin autorización judicial carecen de todo valor probatorio, sin que el Poder Revisor de la Constitución haya establecido alguna excepción a la consecuencia de vulnerar ese precepto fundamental, debe estimarse que la imposibilidad constitucional de otorgar algún valor probatorio a esas grabaciones opera plenamente en el caso del procedimiento indagatorio previsto en el artículo 97, párrafo segundo, de la propia Constitución, aunque éste no tenga el carácter de un procedimiento jurisdiccional, pues aun cuando no está sujeto al rigorismo propio de éste sí lo está al respeto irrestricto de los derechos fundamentales consagrados en esa Ley Fundamental.12

Facultad de investigación de violaciones graves de garantías individuales 2/2006*. Solicitantes: Cámaras de Diputados y de Senadores del Congreso de la Unión. 29 de noviembre de 2007. Mayoría de ocho votos. Ausente: José Fernando Franco González Salas. Disidentes: José Ramón Cossío Díaz y Genaro David Góngora Pimentel. Dictaminador: Juan N. Silva Meza. Encargado del engrose: Sergio Salvador Aguirre Anguiano. Secretario: Luis Fernando Angulo Jacobo. El Tribunal Pleno, el veintiséis de febrero en curso, aprobó, con el número XXXI/2008, la tesis aislada que antecede. México, Distrito Federal, a veintiséis de febrero de dos mil ocho. *Dictamen que valora la investigación constitucional realizada por la comisión designada en el expediente 2/2006, integrado con motivo de las solicitudes formuladas por las Cámaras de Diputados y de Senadores del Congreso de la Unión, para investigar violaciones graves de garantías individuales.

En esta tesis la Suprema Corte establece que una injerencia violatoria del derecho a la privacidad de las comunicaciones consagrado en la Constitución debe de proceder de una autoridad. Por lo tanto, si un particular procede de dicha manera no está constituyendo una violación a la comunicación privada:

> COMUNICACIONES PRIVADAS. LA ADMISIÓN DE LA PRUEBA DOCUMENTAL DE SUS GRABACIONES NO INFRINGE LA GARANTÍA DE SU INVIOLABILIDAD.- Los artículos contenidos en el capítulo I, título primero "De las garantías individuales", de la Constitución Federal, protegen los derechos subjetivos del gobernado reconocidos por la ley frente a los actos de las autoridades; por tanto, de acuerdo con lo dispuesto por los párrafos noveno y décimo del artículo 16 de nuestra Carta Magna, para que se actualice la hipótesis de una violación a la intervención de comunicaciones privadas, el acto mismo de la intervención de cualquier comunicación privada necesariamente debe provenir de una autoridad y nunca de un particular, siempre que no se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral, administrativo, ni en el caso de las comunicaciones del detenido con su defensor; de manera que como en la especie se trata de materia civil y, especialmente, no existió ningún acto de autoridad federal mediante el cual se interviniera la comunicación telefónica sostenida entre el quejoso y la cónyuge

12. [TA]Tesis: P. XXXI/2008, Semanario Judicial de la Federación y su Gaceta. Novena Época, t. XXVII, Abril de 2008, página 5, Registro número 169884.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

del tercero perjudicado recurrente, sino que tal intervención se llevó a cabo por éste último mediante la grabación realizada en el teléfono instalado en su domicilio, es decir, en su propia línea telefónica, con el aparato comúnmente llamado contestadora o grabadora de recados, no es cierto que la admisión de la prueba documental de audiocintas y su inspección judicial que ofreció el referido recurrente, así como su recepción y reproducción material, infrinja en perjuicio del quejoso la garantía relativa a la inviolabilidad de las conversaciones privadas que consagra el artículo 16 de la Constitución Federal.13

Nota: Por instrucciones del Tribunal Colegiado de Circuito, esta tesis se publicó nuevamente con la modificación en el precedente que el propio tribunal ordenó, para quedar como aparece publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XXVIII, diciembre de 2008, página 984, con el rubro: "COMUNICACIONES PRIVADAS. LA ADMISIÓN DE LA PRUEBA DOCUMENTAL DE SUS GRABACIONES NO INFRINGE LA GARANTÍA DE SU INVIOLABILIDAD."

Más de una década después, una tesis reconoce que cuando un particular realiza la intervención de alguna comunicación privada, ésta sí constituye una infracción a la norma fundamental pues las comunicaciones privadas son inviolables y la consecuencia es que estas no pueden ser admitidas como medio de prueba en un procedimiento. El Tribunal señala contundentemente que estos actos constituyen una ilicitud constitucional.

De acuerdo a este criterio, la grabación de alguna comunicación privada llevada a cabo por un particular trae por consecuencia una ilicitud constitucional, de conformidad con la primera parte del párrafo noveno del artículo 16 constitucional que establece como principio universal que: "Las comunicaciones privadas son inviolables...". En este tenor, este tipo de grabaciones telefónicas no pueden ser admitidas como medio de prueba en un procedimiento, pues al haberse obtenido a través de una conducta que constituye un ilícito constitucional, resulta evidente que se trata de pruebas contrarias a derecho que vulneran la norma constitucional así como la adjetiva. En este sentido, para conocer la verdad sobre los puntos controvertidos, el juzgador puede valerse de cualquier persona, cosa o documento, sin más limitación que la consistente en que las pruebas no estén prohibidas por la ley ni sean contrarias a la moral. Esta es la transcripción:

GRABACIONES TELEFÓNICAS OBTENIDAS POR UN PARTICULAR FUERA DE LOS CASOS PERMITIDOS POR EL ARTÍCULO 16 DE LA CONSTITUCIÓN FEDERAL. CONSTITUYEN UNA PRUEBA CONTRARIA A DERECHO QUE NO DEBE SER ADMITIDA (LEGISLACIÓN DEL ESTADO DE QUERÉTARO).- Del análisis del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos y de la exposición de motivos de la reforma efectuada a dicho numeral el día tres de julio de mil novecientos noventa y seis, se advierte que la intervención de los medios de comunicación privada únicamente está permitida como una estrategia para combatir el crimen organizado, en los términos y con las condiciones que el propio numeral establece; sin embargo, cuando un particular realiza la intervención de alguna comunicación privada, ésta entraña una ilicitud constitucional, pues

13. [TA] Tesis: I.5o.C.9 K, Semanario Judicial de la Federación y su Gaceta, Tribunales Colegiados de Circuito, Novena Época, t. VI, diciembre de 1997, p. 656, Registro número 197343.

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

> la primera parte del párrafo noveno del referido artículo 16 establece como principio universal que: "Las comunicaciones privadas son inviolables..."; en consecuencia, las grabaciones telefónicas obtenidas fuera de los casos que prevé el invocado numeral, no pueden ser admitidas como medio de prueba en un procedimiento, porque al haberse obtenido a través de una conducta que entraña un ilícito constitucional, resulta evidente que se trata de pruebas contrarias a derecho, lo cual, vulnera no sólo la citada norma constitucional, sino lo que señala el artículo 266 del Código de Procedimientos Civiles del Estado de Querétaro, en cuanto a que, para conocer la verdad sobre los puntos controvertidos, el juzgador puede valerse de cualquier persona, cosa o documento, sin más limitación que la consistente en que las pruebas no estén prohibidas por la ley ni sean contrarias a la moral.14

De acuerdo al siguiente razonamiento de los Tribunales Colegiados de Circuito, el contenido de las pertenencias de un detenido no está sujeto a protección. Es por ello que sí se puede utilizar la información obtenida de un teléfono móvil que se esté en posesión de un detenido sujeto a investigación del Estado, quedando a discreción del órgano jurisdiccional el valor que le otorgue a estos elementos de prueba. Un análisis reflexivo de esta tesis sugiere que no es consistente con el artículo 16 de la Constitución. Meses más tarde, con una contradicción de tesis –y con un criterio garantista—, se resuelve que la protección de la privacidad se amplía a los datos guardados en un teléfono celular por lo que éstos no pueden ser utilizados en contra de una persona. Se transcribe el primer criterio a que hacemos mención:

> INTERVENCIÓN DE COMUNICACIONES PRIVADAS. NO LA CONSTITUYE EL HECHO DE QUE EL MINISTERIO PÚBLICO INDAGUE SOBRE LA INFORMACIÓN QUE CONTIENEN LOS TELÉFONOS CELULARES RELACIONADOS CON LA COMISIÓN DE UN DELITO.- La revisión de la información contenida en los teléfonos celulares relacionados con la comisión de un delito no constituye una intervención de comunicaciones privadas, cuya inviolabilidad preserva el artículo 16 de la Constitución Federal y, por tanto, no se requiere del consentimiento de los inculpados para que la autoridad investigadora indague la información que contienen, toda vez que al tratarse del aseguramiento de los objetos que aquéllos llevaban consigo el día de su aprehensión, procede que la representación social realice sobre los aparatos telefónicos las pruebas que estime pertinentes para el debido esclarecimiento de los hechos a que se contrae la causa penal de origen, y así, la autoridad judicial pueda otorgarles el valor que les corresponda conforme a las normas procesales aplicables.15
>
> SEGUNDO TRIBUNAL COLEGIADO EN MATERIAS PENAL Y ADMINISTRATIVA DEL DÉCIMO SÉPTIMO CIRCUITO.
>
> Amparo directo 9/2010. 17 de marzo de 2011. Unanimidad de votos. Ponente: Marco Antonio Rivera Corella. Secretaria: Araceli Delgado Holguín.
>
> Nota: Esta tesis fue objeto de la denuncia relativa a la contradicción de tesis 194/2012, de la que derivó la tesis jurisprudencial 1a./J. 115/2012 (10a.) de rubro: "DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE

14. TA] tesis: XXII.2o.21 C, Semanario Judicial de la Federación y su Gaceta, Tribunales Colegiados de Circuito, Novena Época, t. XXVIII, septiembre de 2008, p. 1273, Registro número 168917.

15. [TA] Tesis XVII.2o.P.A.37 P, Semanario Judicial de la Federación y su Gaceta, Tribunales Colegiados de Circuito, Novena Época, t. XXXIII, junio de 2011, p. 1482, Registro número 161828.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

EXTIENDE A LOS DATOS ALMACENADOS EN ELTELÉFONO MÓVIL ASEGURADO A UNA PERSONA DETENIDA Y SUJETA A INVESTIGACIÓN POR LA POSIBLE COMISIÓN DE UN DELITO."

Los dispositivos electrónicos que son producto de la evolución tecnológica y que se utilizan para sostener comunicaciones deben de ser protegidas por el derecho a la inviolabilidad de las comunicaciones privadas consagrado por el artículo 16 de la Constitución Federal. Sin embargo, de acuerdo al criterio de los Tribunales Colegiados de Circuito si el ministerio público ordena extraer la información contenida en un teléfono móvil que fue asegurado por estar abandonado en el lugar probable de la comisión de un delito y sin que exista detenido alguno, no vulnera dicho derecho protegido. En su razonamiento, el Tribunal explica que esta prerrogativa no se transgrede por el hecho de que un teléfono celular que se encuentre abandonado en el lugar probable de la comisión de un ilícito y sea asegurado para investigar los datos que se encuentren en este. Ello en razón de que la protección a la información pertenece exclusivamente a la intimidad de la persona titular del derecho protegido, no existiendo en esta hipótesis algún titular. Luego entonces, la información no es considerada como ilícita pues no implica violación al derecho fundamental a la inviolabilidad de la comunicación privada. He aquí el criterio:

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SI EL MINISTERIO PÚBLICO ORDENA EXTRAER LA INFORMACIÓN CONTENIDA EN UN TELÉFONO CELULAR QUE FUE ASEGURADO POR ESTAR ABANDONADO EN EL LUGAR PROBABLE DE LA COMISIÓN DE UN DELITO Y SIN QUE EXISTA DETENIDO ALGUNO, NO VIOLA DICHA PRERROGATIVA FUNDAMENTAL.- Conforme al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, todas las formas existentes de comunicación y las que son fruto de la evolución tecnológica, deben protegerse por el derecho fundamental a su inviolabilidad. Al respecto, la Primera Sala de la Suprema Corte de Justicia de la Nación en la jurisprudencia 1a./J. 115/2012 (10a.), estableció que ese derecho se extiende a los datos almacenados en los teléfonos móviles que son asegurados a las personas detenidas sujetas a investigación por la posible comisión de un delito; aparatos en los que se guarda información privada, ya sea en forma de texto, audio, imagen o video, y de la cual la autoridad investigadora para tener acceso a ella, debe solicitar a un Juez la intervención de la comunicación privada conforme al texto constitucional en cita. Sin embargo, cuando el Ministerio Público ordena extraer la información contenida en un teléfono celular que es asegurado por encontrarse abandonado en el lugar probable de la comisión de un delito y sin que exista detenido alguno, no viola esta prerrogativa fundamental, pues la protección a la información pertenece exclusivamente a la intimidad de la persona titular del derecho protegido, por lo que si en el caso real y concreto no existe algún titular, por no haber detenido con motivo de los hechos o poseedor identificado de éste, es incuestionable que el Ministerio Público, conforme a sus facultades de investigación del delito en términos del artículo 21 constitucional, está facultado para ordenar la extracción de la información almacenada sin que medie la solicitud correspondiente a la autoridad judicial, un teléfono celular que es asegurado por encontrarse abandonado en el lugar probable de la comisión de un delito y sin que exista detenido alguno, no viola esta prerrogativa fundamental, pues la protección a la información pertenece exclusivamente a la intimidad de la persona titular del derecho protegido, por lo que si en el caso real y concreto no existe algún titular, lo cual no implica violación al

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

derecho fundamental a la inviolabilidad de la comunicación privada y, por ende, que esa información no sea considerada como ilícita, en razón de que las pruebas obtenidas a partir de ésta, no serían esencialmente causa de los datos obtenidos, sino que derivarían de la facultad constitucional de la investigación realizada.16

NOVENO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO. AMPARO EN REVISIÓN 244/2012. 7 de febrero de 2012. Mayoría de votos. Disidente: Guadalupe Olga Mejía Sánchez. Ponente: Emma Meza Fonseca. Secretaria: María del Carmen Campos Bedolla.

Nota: La tesis de jurisprudencia 1a./J. 115/2012 (10a.) citada, aparece publicada en el Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro XVII, Tomo 1, febrero de 2013, página 431, con el rubro: "DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE EXTIENDE A LOS DATOS ALMACENADOS EN EL TELÉFONO MÓVIL ASEGURADO A UNA PERSONA DETENIDA Y SUJETA A INVESTIGACIÓN POR LA POSIBLE COMISIÓN DE UN DELITO."

Continuando con el tema de la telefonía móvil, la Primera Sala de la Suprema Corte de Justicia de la Nación ha sostenido que el teléfono celular en el que se resguarda información es clasificada como privada y la protección del derecho a la inviolabilidad de las comunicaciones privadas se extiende a los datos almacenados en tal dispositivo, ya sea que se contenga en texto, audio, imagen o video. En este escenario, la jurisprudencia señala que el derecho a la inviolabilidad de las comunicaciones comprende los datos guardados en el dispositivo móvil asegurado a una persona detenida y sujeta a investigación por la posible comisión de un delito. Ahora bien, si se realiza esa actividad, el Ministerio Público debe solicitar autorización judicial para intervenir el teléfono y en ese sentido, cualquier prueba que se extraiga sin dicha orden judicial o la que derive de ésta, será considerada como ilícita y no tendrá valor probatorio dentro de un juicio. Se transcribe a continuación:

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE EXTIENDE A LOS DATOS ALMACENADOS EN EL TELÉFONO MÓVIL ASEGURADO A UNA PERSONA DETENIDA Y SUJETA A INVESTIGACIÓN POR LA POSIBLE COMISIÓN DE UN DELITO.- En términos del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para intervenir una comunicación privada se requiere autorización exclusiva de la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, por lo que todas las formas existentes de comunicación y las que son fruto de la evolución tecnológica deben protegerse por el derecho fundamental a su inviolabilidad, como sucede con el teléfono móvil en el que se guarda información clasificada como privada por la Primera Sala de la Suprema Corte de Justicia de la Nación; de ahí que el ámbito de protección del derecho a la inviolabilidad de las comunicaciones privadas se extiende a los datos almacenados en tal dispositivo, ya sea en forma de texto, audio, imagen o video. Por lo anterior, no existe razón para restringir ese derecho a cualquier persona por la sola circunstancia de haber sido detenida y estar sujeta a investigación por la posible comisión de un delito, de manera que si la autoridad encargada de la investigación, al detenerla, advierte que trae consigo un teléfono móvil, está facultada

16. [TA] Tesis: I.9o.P.25 P (10a.), Semanario Judicial de la Federación y su Gaceta, Tribunales Colegiados de Circuito, Décima Época, t. 3, libro XIX, abril de 2013, p. 2108. Registro 2003266

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

para decretar su aseguramiento y solicitar a la autoridad judicial la intervención de las comunicaciones privadas conforme al citado artículo 16 constitucional; sin embargo, si se realiza esa actividad sin autorización judicial, cualquier prueba que se extraiga, o bien, la que derive de ésta, será considerada como ilícita y no tendrá valor jurídico alguno.17

CONTRADICCIÓN DE TESIS 194/2012. Entre las sustentadas por el Segundo Tribunal Colegiado en Materias Penal y Administrativa del Décimo Séptimo Circuito y el Cuarto Tribunal Colegiado del Décimo Octavo Circuito. 10 de octubre de 2012. La votación se dividió en dos partes: mayoría de cuatro votos por lo que se refiere a la competencia. Disidente: José Ramón Cossío Díaz. Unanimidad de cinco votos en cuanto al fondo. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Jorge Antonio Medina Gaona.

Tesis de jurisprudencia 115/2012 (10a.). Aprobada por la Primera Sala de este Alto Tribunal, en sesión de fecha diecisiete de octubre de dos mil doce.

La Primera Sala de la Suprema Corte dispuso que aun cuando un dispositivo de comunicación inalámbrico se encuentre abandonado, si la autoridad sospecha que contiene información relacionada con algún ilícito, para efecto de extraer los datos allí almacenados se debe de obtener autorización del juez federal. De otra manera, se estará transgrediendo el derecho a la privacidad consagrado en la constitución. Este es el criterio:

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE EXTIENDE A TELÉFONOS O APARATOS DE COMUNICACIÓN ABANDONADOS O RESPECTO DE LOS CUALES NO SE TENGA CONOCIMIENTO DE QUIÉN ES SU TITULAR, POR LO QUE PARA ACCEDER A SU INFORMACIÓN DEBE SOLICITARSE LA AUTORIZACIÓN DE UN JUZGADOR FEDERAL. Esta Primera Sala de la Suprema Corte de Justicia de la Nación ha sostenido que todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, deben protegerse por el derecho fundamental a la inviolabilidad de las comunicaciones privadas; así, lo que está prohibido por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos es la intercepción o el conocimiento antijurídico de una comunicación ajena realizada por particulares o por alguna autoridad. Ahora bien, la violación del derecho referido se consuma en el momento en que se escucha, graba, almacena, lee o registra –sin el consentimiento de los interlocutores– una comunicación ajena, con independencia de que con posterioridad se difunda el contenido de la conversación interceptada. En estas condiciones, para que sea constitucional la intervención de cualquier comunicación privada, en términos del referido artículo, deberá existir, indefectiblemente, control judicial previo por parte de un juzgador integrante del Poder Judicial de la Federación. Consecuentemente, al poseer el derecho a la inviolabilidad de las comunicaciones privadas autonomía propia y al configurar una garantía formal que protege las comunicaciones con independencia de su contenido, éste se extiende a teléfonos o aparatos de comunicaciones abandonados o respecto de los cuales no se tenga conocimiento de quién es su titular, por lo que la autoridad competente deberá solicitar la autorización de un juzgador federal para acceder a la información contenida en un aparato de comunicación en dichos supuestos. Lo anterior se justifica, porque la única excepción

17. Tesis: 1a./J. 115/2012 (10a.), Semanario Judicial de la Federación y su Gaceta, Primera Sala, Décima Época, t. 1, Libro XVII, febrero de 2013, p. 431. Registro número 2002741

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

para que no exista control judicial previo para intervenir algún tipo de comunicación privada, es que alguno de los participantes en la comunicación aporte la información a las autoridades competentes voluntariamente. 18

Amparo directo en revisión 3506/2014. 3 de junio de 2015. Cinco votos de los Ministros Arturo Zaldívar Lelo de Larrea, José Ramón Cossío Díaz, Jorge Mario Pardo Rebolledo, Olga Sánchez Cordero de García Villegas y Alfredo Gutiérrez Ortiz Mena. Los Ministros Zaldívar, Pardo, Sánchez Cordero y Gutiérrez, reservaron su derecho para formular voto concurrente. Ponente: José Ramón Cossío Díaz. Secretaria: Rosalba Rodríguez Mireles.

Este criterio estableced que aun tratándose de la investigación por un caso de delincuencia organizada, se debe de obtener autorización del juez federal para intervenir una comunicación debido a que éstas están protegidas a nivel constitucional. Se transcribe a continuación:

COMUNICACIONES PRIVADAS. DEBE EXISTIR UNA AUTORIZACIÓN JUDICIAL PARA INTERVENIRLAS, AUN EN CASOS DE INVESTIGACIÓN SOBRE DELINCUENCIA ORGANIZADA. Para intervenir una comunicación privada se requiere autorización exclusiva de la autoridad judicial federal, a petición de la que faculte la ley o del titular del Ministerio Público, por lo que todas las formas existentes de comunicación –como las realizadas a través del teléfono celular– y aquellas que sean fruto de la evolución tecnológica, así como los datos almacenados en los diferentes dispositivos, están protegidas por el derecho fundamental a su inviolabilidad. De ahí que si la intervención de las comunicaciones privadas se realiza sin una autorización judicial, cualquier prueba extraída, o bien, derivada de ésta, será considerada como ilícita y no tendrá valor jurídico alguno. Por tanto, esta Primera Sala de la Suprema Corte de Justicia de la Nación no encuentra razón suficiente para que, aun en una investigación sobre delincuencia organizada, no se cumpla con el requisito de que sólo con orden judicial puede analizarse la información contenida en los medios de comunicación. 19

Amparo en revisión 338/2012. 28 de enero de 2015. Cinco votos de los Ministros Arturo Zaldívar Lelo de Larrea, José Ramón Cossío Díaz, Jorge Mario Pardo Rebolledo, quien formuló voto concurrente, Olga Sánchez Cordero de García Villegas y Alfredo Gutiérrez Ortiz Mena. Ponente: Alfredo Gutiérrez Ortiz Mena. Secretaria: Karla I. Quintana Osuna.

Como se puede observar, la evolución de los criterios de la Suprema Corte de Justicia contempla la protección de las comunicaciones, imágenes, audios, videos y otra información almacenada en teléfonos inalámbricos pues su utilización va en aumento.

XII. Tecnología, medios probatorios y derechos fundamentales

En la actualidad en los Estados democráticos la investigación de un delito y los medios probatorios que se utilicen con este propósito deben de tutelar los derechos fundamentales de los individuos investigados. En ese sentido, el poder de persecución e investigación

18. TA Tesis1a. CCLIII/2015 (10a.), Gaceta del Semanario Judicial de la Federación. Décima Epoca, t. 1, Libro 21, Agosto de 2015, pag 465. Registro número 2009820

19. TA 1a. CCCXXV/2015 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Epoca, t. 1, Noviembre del 2015, página 960. Registro número 2010347.

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

criminal que tiene el Estado no es absoluto sino que debe de estar acotado y evitar actos arbitrarios, sin fundamentación y no proporcionales al hecho investigado. Dino (2018) ha referido que únicamente así se podrá mantener un equilibrio entre la búsqueda de la verdad y los derechos fundamentales. Los mismos ordenamientos a saber, la Constitución, los códigos de procedimientos penales e incluso los protocolos de investigación deben de fijar requisitos mínimos para las actuaciones de la autoridad, es así como se podrá hablar de un debido proceso y de garantías en el proceso penal. García Ramírez (2016) señala que el debido proceso, es el desarrollo de un proceso judicial conforme a todas las garantías y aplicación de reglas jurídicas, que presuponen el acceso a la justicia, constituyendo un derecho sustantivo, formal y cualitativo.

Las modernas técnicas de captación de conversaciones privadas a través de la instalación de aparatos de escucha y grabación, tales como micrófonos ocultos, hacen posible escuchar las conversaciones al interior de domicilios particulares o bien intervenir teléfonos móviles.

Para que el contenido de una intervención de comunicaciones pueda ser considerada como prueba dentro de un procedimiento judicial ésta debe de cumplir con los siguientes requisitos:

- Que la intervención esté prevista dentro de un ordenamiento jurídico
- Que sea una medida necesaria para proteger bienes como seguridad nacional o pública así como derechos y libertades de los demás.
- Que sea necesaria la intervención y proporcionalidad a la conducta ilícita investigada.

En esta línea, una decisión judicial justa es aquella en la que para la búsqueda y establecimiento de la verdad se utilizaron medios y métodos lícitos, apegados a la norma y controlados o autorizados por un funcionario judicial.

XIII. Conclusiones

Frente a los medios tradicionales que han perdido utilidad práctica y vigencia, han surgido nuevas formas de comprobar actos realizados por y a través de las tecnologías. Desde esta perspectiva, a medida que una gran cantidad de actos se realizan con medios informáticos, se ha llegado a considerar que los documentos tradicionales están perdiendo utilidad práctica y vigencia.

La revolución tecnológica ha evolucionado el mundo jurídico, causando un gran impacto en el ámbito probatorio pues han surgido medios de convicción digitales o electrónicos que suponen nuevas formas en su obtención, procesamiento y valoración y que por lo tanto, también requieren ser incluidos en una normativa actualizada conforme a las especificidades de este tipo de acervo probatorio.

La intervención de comunicaciones, que en el caso mexicano se permite para la investigación de casos de delincuencia organizada, supone la utilización de medios digitales para su obtención. Este tipo de injerencias constituyen una transgresión a la intimidad personal y al secreto en las comunicaciones. La normativa sin embargo es escueta sien-

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07

do omisa en varios aspectos por ejemplo, se necesita establecer que las autoridades que practican la intervención tienen la obligación de entregar la totalidad de la cinta que fue grabada y que queda prohibido seleccionar o desechar partes de las conversaciones pues esto se traduce en sospecha de posible adulteración. Con respecto a este tema, los criterios de la Suprema Corte de Justicia, establecen los casos en que la intervención de dispositivos no constituye una trasgresión a derechos fundamentales.

En suma, el ritmo de desarrollo acelerado de la tecnología hace que el derecho tenga que evolucionar rápidamente para estar a la vanguardia de tal forma que exista aproximación entre tecnología y proceso.

Bibliografía

Arazi, R. (2008). *Prueba ilícita y prueba científica*. Rubinzal Culzoni editores. p. 29

Caro Coria, D. (2006). *Las garantías constitucionales del proceso penal*, disponible en https://bit.ly/2GuYkb2

Cossío, J. et al. (2017). *El uso de evidencia científica y opinión experta en las sentencias de la Suprema Corte de Justicia de la Nación*. México. Tirant lo Blanch. p. 5.

Rodríguez Mourillo, J. et al. *Derecho penal e internet. En Régimen Jurídico de internet*. Madrid. Editorial la Ley. Colección de Derecho de las Comunicaciones. pp. 288, 289.

Cremades García, J., Fernández Ordóñez, M. A., & Illescas Ortiz, R. (2009). Régimen jurídico de internet/coordinadores, Javier Cremades, Miguel Angel Fernández-Ordóñez, Rafael Illescas.

De la Rosa, P. (2019). *Las tecnologías, el ciberespacio y el derecho penal.* Editorial Porrúa.

De Urbano Castillo E. (2009). *La valoración de la prueba electrónica*. Valencia. Tirant Lo Blanch. p.54.

Delgado Martín, J. (2017). *La prueba digital. Concepto, clases, aportación al proceso y valoración*, Diario la ley, no. 6, sección ciberderecho, España. editorial Wolters Kluwer.

García Ramírez, S. (2016). *El debido proceso. Criterios de la jurisprudencia interamericana*. México. Porrúa. 3 ed., 2016, p. 14-16.

Goodman M. (2003). *Cibercriminalidad,* INACIPE. p. 8.

INEGI. (2019). Censo nacional de impartición de justicia federal 2018.

Jijena, R. & Valdés, T. (2003). El derecho y la sociedad de la información la importancia de internet en el mundo actual. México. Tec de Monterrey. 4 (67) p.12.

López Alonso, C. (2006). El correo electrónico. *Estudios de lingüística del español*, vol.24.

Lucas, A. S., Cassany, D., Fretes, G., Knobel, M., Lankshear, C., Meneses, J. & Sigalés, C. (2014). *Sociedad del conocimiento, tecnología y educación*. Ediciones Morata.

Muñoz Conde, F. (2008). De las prohibiciones probatorias al Derecho procesal penal del enemigo, editorial hammurabi. p. 68. Núñez Jover, J. (1989). *"Ciencia, Tecnología y Sociedad", Problemas Sociales de la Ciencia y la Tecnología.* La Habana. GESOCYT. Editorial Félix Varela.

Parra, J. (2006). *Manual de Derecho Probatorio.* Colombia. Ediciones LTDA. p. 73.

Pico i Junoy, J. (2017). Presentación de *Peritaje y prueba pericial*. Barcelona. Bosh.

Ruiz Jaramillo, L. (2007). El derecho a la prueba como un derecho fundamental. Facultad de Derecho y Ciencias Políticas. Universidad de Antioquia. 64, nº 143 p. 188.

Yáñez, I. C., Zermeño, M. G. G., & Chávez, M. M. P. (2015). Competencias digitales en el estudiante adulto trabajador. *Revista Interamericana de Educación de Adultos*, *37*(2), 10-24.

Vaquera, M. L. C., & María, L. (2014). El discurso del WhatsApp: entre el Messenger y el SMS. *Oralia*, *17*, 85-114.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 109-128
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.07