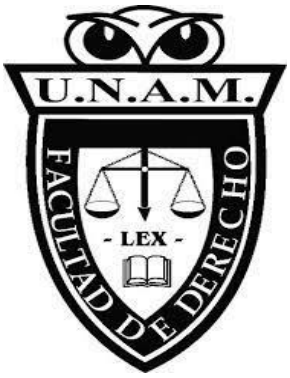
VNIVERSIDAD NACIONAL
AVTNOMA DE
MEXICO



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE POSGRADO EN DERECHO

LAS INTERVENCIONES DE COMUNICACIONES PRIVADAS EN EL MARCO JURÍDICO MEXICANO

TESIS QUE PARA OPTAR POR EL GRADO DE:

ESPECIALISTA EN DERECHO PENAL

PRESENTA:

JOSUÉ ÁNGEL GONZÁLEZ TORRES

TUTORA PRINCIPAL:

DRA. ZORAIDA GARCÍA CASTILLO

ESCUELA NACIONAL DE CIENCIAS FORENSES

INTEGRANTES DEL SÍNODO:

DRA. MARÍA TERESA AMBROSIO MORALES

DRA. CLARA LUZ ÁLVAREZ GONZÁLEZ DE CASTILLA

DR. ARTURO MANSILLA OLIVARES

MTRO. JESÚS BECERRA PEDROTE

CIUDAD UNIVERSITARIA, MÉXICO, 2024

Página intencionalmente dejada en blanco.

Índice

Agradecimientos

La presente investigación es en buena medida resultado de la asesoría y apoyo de los miembros del sínodo. Agradezco a mi tutora principal, Dra. Zoraida García Castillo quien aportó agudos puntos de vista para mejorar el contenido de la investigación y por su presencia acuciosa en todo el momento en el desarrollo la tesina.

Mi gratitud a las y los integrantes del sínodo: Dra. María Teresa Ambrosio Morales, Dra. Clara Luz Álvarez González De Castilla, Dr. Arturo Mansilla Olivares y Mtro. Jesús Becerra Pedrote, quienes revisaron la investigación, formularon críticas, comentarios, puntualizaciones y realizaron planteamientos y aportaciones de bibliografía para mejorar el documento.

No obstante, todos y cada uno de los argumentos, afirmaciones e incorrecciones contenidas a lo largo del documento son responsabilidad directa del autor y no de los docentes mencionados ni de las instituciones involucradas.

Agradezco y reconozco al Programa de Posgrado en Derecho de la Universidad Nacional Autónoma de México por el apoyo durante todos estos años y por fungir como una de las principales casas de conocimiento en el ámbito jurídico a nivel nacional.

Página intencionalmente dejada en blanco.

Dedicatorias

- A mis padres, Agustín González, María Guadalupe Torres y a mi hermano, Jonathan González. Gracias por su comprensión, afecto y ánimo. A ustedes les debo cada uno de los logros obtenidos.

- A la memoria de mis abuelos, que son motivo de orgullo personal.

- A mis tíos, Javier y Jesús Torres por su constante presencia e impulso en mi desarrollo personal, académico y profesional. En general a mi familia por todo lo que me han brindado.

- A los profesores a lo largo de toda mi formación académica, por compartir su conocimiento y por formar a las nuevas generaciones.

- A mis amigos a lo largo de estos años, especialmente con quienes compartí aulas en la ENP 5 “José Vasconcelos”, Facultad de Ciencias Políticas y Sociales y Facultad de Derecho de la UNAM, por hacer la vida más llevadera en todos los sentidos.

- A mi *alma mater*, la UNAM, por cambiar realidades y por ser un impulso para la mejora constante de la sociedad mexicana. Una responsabilidad y un orgullo pertenecer a la máxima casa de estudios de México. Con ella una amplísima deuda.

- A mis colegas y jefes en CNS, SIE, UNAM, SSPC, CNI e ITAM.

- A todos los buenos elementos y a los héroes anónimos de las instituciones de seguridad, defensa y procuración de justicia que defienden con honradez, integridad y dignidad la vida, la integridad y el patrimonio de las personas.

Página intencionalmente dejada en blanco.

Siglas y abreviaturas

Sigla / abreviatura	Significado
AIC	Agencia de Investigación Criminal de la FGR
ASF	Auditoría Superior de la Federación
CENTRO NACIONAL	Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones del PJF
CFIC	Centro Federal de Inteligencia Criminal de la FGR
CIDH	Comisión Interamericana de Derechos Humanos
CIM	Centro de Inteligencia Militar de la SEDENA
CISEN	Centro de Investigación y Seguridad Nacional (ahora CNI)
CJM	Centro de Justicia Militar
CMPP	Código Militar de Procedimientos Penales
CNDH	Comisión Nacional de Derechos Humanos
CNI	Centro Nacional de Inteligencia
CNPP	Código Nacional de Procedimientos Penales
CPEUM	Constitución Política de los Estados Unidos Mexicanos
DOF	Diario Oficial de la Federación
FEMDO	Fiscalía Especializada en Materia de Combate a la Delincuencia Organizada
FGR	Fiscalía General de la República
GN	Guardia Nacional
IFETEL	Instituto Federal de Telecomunicaciones
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
IUN	Unidad de Inteligencia Naval de la SEMAR
PJF	Poder Judicial de la Federación
PGR	Procuraduría General de la República (ahora FGR)
R3D	Red en Defensa de los Derechos Digitales
SCJN	Suprema Corte de Justicia de la Nación
SEDENA	Secretaría de la Defensa Nacional
SEMAR	Secretaría de Marina – Armada de México
SSPC	Secretaría de Seguridad y Protección Ciudadana

Introducción

La presente tesina tiene como objeto de estudio las intervenciones de comunicaciones privadas en su marco jurídico y su uso en instituciones gubernamentales de México. Concretamente, el objetivo central consiste en analizar el uso de las intervenciones de comunicaciones privadas en dependencias de seguridad pública[1], seguridad nacional[2] y procuración de justicia[3] a la luz del marco jurídico, con la finalidad de realizar una serie de recomendaciones para el mejoramiento de éste.

En cada uno de los ámbitos señalados, las intervenciones tienen características particulares y el marco legal es específico, en ese sentido es necesario conocer cuáles son las semejanzas y diferencias.

---

[1] El concepto de "seguridad pública" está definido en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en el artículo 21, de acuerdo con la última reforma del 03 de marzo de 2019, según la cual "…es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en esta constitución y las leyes en la materia. La seguridad pública comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución…". *Vid*. Congreso de la Unión, *Constitución Política de los Estados Unidos Mexicanos*, México, publicada en el Diario Oficial de la Federación el 05 de febrero de 1917, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf [consulta: julio, 2023].

[2] Por su parte, la "seguridad nacional", de acuerdo con el artículo 5 de la Ley de Seguridad Nacional, son las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano. Entre otras, se encuentran la protección frente a riesgos y amenazas, la preservación de la independencia y soberanía nacionales; el mantenimiento de las partes integrantes de la federación; la defensa legítima del Estados mexicano frente a otros Estados; así como la preservación de la democracia, fundada en el desarrollo social y político. Congreso de la Unión, *Ley de Seguridad Nacional*, México, publicada en el Diario Oficial de la Federación el 31 de enero de 2005, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf [consulta: julio, 2023].

[3] Si bien no está definida la "procuración de justicia" como tal, se entiende como la actividad que realiza el estado para investigar, perseguir los delitos y ejercitar la acción penal dentro del marco legal de respeto a los derechos de los ciudadanos. En ese sentido, el artículo 20 constitucional establece las bases del proceso penal acusatorio y oral, y reconoce los principios generales, los derechos de las personas imputadas, y de las víctimas u ofendidos. En tanto, el artículo 21 indica que la "…investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función. El ejercicio de la acción penal ante los tribunales corresponde al Ministerio Público. La ley determinará los casos en que los particulares podrán ejercer la acción penal ante la autoridad judicial…". *Vid. Ibidem*.

Entre las preguntas que plantea esta investigación y que dirigen el texto, se encuentran ¿Cuál es el concepto de intervención de comunicaciones privadas? ¿Cuál es el marco jurídico que las norma? ¿En qué supuestos se puede realizar de acuerdo con la legislación mexicana? ¿Cuáles son los procedimientos para su solicitud e implementación? ¿Qué instituciones pueden utilizarlas y bajo qué parámetros? ¿Es adecuado el marco jurídico actual para los avances en la comunicación y la tecnología? En su caso, ¿Qué se tiene que reformar?

En el país, el máximo ordenamiento jurídico que norma las intervenciones es la Constitución Política de los Estados Unidos Mexicanos (CPEUM). En el artículo 16, párrafos 12, 13 y 15 regula el derecho humano a la inviolabilidad de las comunicaciones privadas. Se señala que se sancionará 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 ella.

El texto constitucional faculta únicamente a los jueces federales para conocer y autorizar las intervenciones a petición del Ministerio Público, autoridad federal facultada o titular del Ministerio Público de las entidades federativas, en el caso de estar relacionadas con la comisión de un delito, el cual podrá ser atendido en el orden común o en el orden federal de acuerdo con las características del mismo.

El escrito que formule el Ministerio Público debe estar debidamente fundado y motivado, y señalar elementos mínimos requeridos por la ley como son: tipo de intervención, sujetos y duración de ésta. Por su parte, el juez de control federal es quien tiene que resolver sobre la petición en forma inmediata y bajo cualquier medio.

Según la Carta Magna, para que la intervención de comunicaciones privadas pueda ser integrada en un juicio y tenga valor probatorio, no debe traspasar los límites establecidos por el marco legal. En caso de no cumplir con los requisitos, se convierte en una prueba ilícita y, por tanto, carece de todo valor probatorio.

La CPEUM, en el artículo 16, como queda patente, se concentra en las intervenciones en materia de procuración de justicia, pero no aborda claramente

aquellas que son reconocidas por las leyes en materia de seguridad nacional y seguridad pública.

Si bien existe un marco jurídico a nivel federal que tiene aplicabilidad nacional, además de una serie de instrumentos normativos locales, se registran una serie de retos importantes. Por ejemplo, en el ámbito de procuración de justicia, la implementación del Sistema de Justicia Penal Acusatorio, entre el 2008 y el 2016, no sólo tuvo como consecuencia la necesidad de que los operadores reaprendieran actividades básicas, sino de enfrentarse a nuevos estándares y técnicas de investigación que no eran utilizadas en el sistema inquisitivo.

Entre otros temas, el sistema de justicia penal acusatorio demandó establecer a las intervenciones como una técnica de investigación relativamente nueva y poco conocida. Permite aportar datos tan relevantes como ubicación de una persona, trazabilidad en movimiento, comunicación con otras personas, posesión de archivos o documentos (imágenes, texto, audio, etc.), comunicación directa con personas involucradas en los hechos y geolocalización en tiempo real, por mencionar algunos aspectos relevantes, que contribuyen al esclarecimiento de un hecho con apariencia de delito.

Al igual que en procuración de justicia, en los ámbitos de seguridad nacional y seguridad pública se han identificado una serie de retos relevantes que ponen a prueba el marco jurídico en la materia. Uno de los claramente identificables y que es común a los tres sectores es el avance tecnológico, pues con el uso de nuevos dispositivos y aplicaciones móviles, así como con la migración de llamadas convencionales a llamadas por internet, la regulación y los dispositivos para realizar las intervenciones quedan obsoletos y se tienen que adaptar a los nuevos escenarios.

En el mismo sentido, es necesario reconocer que, durante el desarrollo de la investigación, se detectó la existencia de intervenciones de comunicaciones que se realizan de manera extrajudicial tanto en el ámbito de la inteligencia como en el ámbito político, así como de un “mercado negro” para la compraventa de diversas

modalidades de intervenciones y tecnologías para su implementación. Sin embargo, estos temas exceden los objetivos planteados en la presente tesina, por lo cual se abordarán únicamente de manera tangencial.

En este contexto, la hipótesis que dirige la investigación sostiene que el marco jurídico actual en la materia es insuficiente para la realización adecuada de acciones de prevención, investigación y persecución de delitos desde las dependencias de seguridad y justicia, por lo que es necesario realizar una revisión profunda del mismo.

Para aprobar o desaprobar esta afirmación, la tesina se divide en cuatro secciones (tres capítulos y un apartado final). En el primer capítulo se indaga sobre el marco jurídico de las intervenciones de comunicaciones privadas que regula su solicitud e implementación a nivel nacional, además de una serie de instrumentos internacionales que tienen o debieran tener aplicabilidad doméstica. Se parte de la Carta Magna pasando por el Código Nacional de Procedimientos Penales, la Ley Orgánica del Poder Judicial de la Federación, el Código Penal Federal, y la Ley Federal de Telecomunicaciones y Radiodifusión, hasta la Ley de Guardia Nacional, la Ley de Seguridad Nacional y La Ley Federal contra la Delincuencia Organizada, por mencionar los principales. Asimismo, se abordan seis instrumentos jurídicos internacionales.

En el segundo capítulo se perfila la definición y la tipología de las intervenciones. Existen cuando menos cuatro definiciones identificadas en la legislación nacional, por lo que se identifican las principales características de ésta. Asimismo, se discuten las cuatro modalidades de intervenciones que son: 1) datos conservados, 2) extracción de información de dispositivos móviles, 3) geolocalizaciones en tiempo real, y 4) escuchas. Cada una de ellas sigue un proceso de solicitud, implementación, análisis de información y objetivos distintos dependiendo la institución donde se desarrollen.

Por su parte, el tercer capítulo identifica justamente las instituciones donde se realizan las intervenciones de comunicaciones privadas en materia de seguridad

pública, seguridad nacional y procuración de justicia. Se argumenta que, en seguridad pública, con la Guardia Nacional (GN), esta herramienta es fundamental para la prevención de delitos federales. En seguridad nacional, a través del Centro Nacional de Inteligencia (CNI) se utilizan con el objetivo de prevenir riesgos y amenazas a la seguridad nacional como terrorismo, traición a la patria, interferencia extranjera en asuntos nacionales, delincuencia organizada, contrainteligencia y afectación a la infraestructura estratégica, entre otras.

Con las Fuerzas Armadas destaca el hecho que carecen de un marco jurídico para implementar este tipo de técnicas en el ámbito civil. Este argumento se desarrollará a lo largo de la investigación.

Mientras que, en procuración de justicia, por conducto de la Fiscalía General de la República (FGR) y las fiscalías y procuradurías locales, son actos de investigación útiles para la investigación ministerial y para la integración de datos en Carpetas de Investigación. En cualquiera de los ámbitos enunciados, se requiere un control judicial por parte de los jueces adscritos al Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones. También se plantea una breve discusión sobre el concepto de "espionaje" y su actualidad en México.

En la cuarta sección se formulan una serie de recomendaciones concretas de acuerdo con el análisis realizado para fortalecer el marco jurídico en diversos rubros: definición de concepto, modalidades y procesos de aplicación; robustecimiento del marco jurídico para la actuación de las instituciones de seguridad pública y seguridad nacional para dar certidumbre en su actuación, dado que existen márgenes muy importantes para la acción discrecional, especialmente con las Fuerzas Armadas; y adaptación del marco legal a la evolución tecnológica y de telecomunicaciones que es dinámica y cambiante.

Es importante decir que una de las principales motivaciones para la realización de esta investigación es que no se cuenta con suficiente literatura especializada en la materia. Existen aproximaciones generales desde el ámbito académico que plantea

una descripción jurídica o revisiones estadísticas del número de intervenciones en instituciones de seguridad y justicia, pero se carece de un estudio que aborde la complejidad de las intervenciones en diversas instituciones y enfoques del país. En ese sentido, aspira a ser una contribución a la literatura especializada.

Finalmente, es necesario realizar tres acotaciones antes del desarrollo del capitulado. Primero, el documento es una investigación original producto de la información pública disponible. Segundo, la tesina se acota temáticamente al estudio de las dependencias federales y no de las secretarías ni fiscalías locales, tema que implica una investigación en sí misma por la complejidad. Y, tercero, todas las afirmaciones e incorrecciones contenidas son responsabilidad del autor y no de los tutores y revisores de la tesina, instituciones o dependencias nacionales o extranjeras que pudieran estar relacionadas directa o indirectamente.

Capítulo 1. Marco jurídico de las Intervenciones de Comunicaciones Privada en México.

En el primer capítulo se indaga sobre el marco jurídico de las intervenciones de comunicaciones privadas que regula su solicitud e implementación a nivel federal, como revisión fundamental en los ámbitos de procuración de justicia, seguridad pública y seguridad nacional. Posteriormente, se abordan nueve instrumentos nacionales y seis ordenamientos internacionales relacionados directa e indirectamente con el objeto de estudio de la tesina. A continuación se presentan los principales hallazgos.

1.1. Legislación nacional

Esta sección parte de la CPEUM que, al ser el máximo ordenamiento jurídico del país, establece el marco general de donde se desprende todo el enramado relacionado con las intervenciones de comunicaciones privadas. Es el fundamento de las intervenciones en el ámbito de la procuración de justicia, la seguridad pública y la seguridad nacional.

1.1.1. Constitución Política de los Estados Unidos Mexicanos (CPEUM)[4]

En la CPEUM, artículo 16, párrafo 12, se garantiza el derecho a la inviolabilidad de las comunicaciones privadas. Es la piedra angular de las intervenciones en la medida en que señala que se sancionará penalmente cualquier tipo de acto que atente contra la libertad y privacía de las mismas. El párrafo 13 del mismo artículo mandata que:

> *"…[Es] exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente,*

[4] Congreso de la Unión, *Constitución Política de los Estados Unidos Mexicanos*, *Óp. Cit*.

quien podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración…".

Igualmente, establece una serie de limitaciones al indicar que no será posible otorgar las autorizaciones cuando se trate de materia electoral, fiscal, mercantil, civil, laboral o administrativo ni en el caso de las comunicaciones del detenido con su defensor.

En el párrafo 14 señala que los Poderes Judiciales, haciendo referencia a los federales y locales, contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio las técnicas de investigación que requieran control judicial. Aunque no se abordan específicamente las intervenciones de comunicaciones privadas, se entiende que quedan incluidas.

Mientras que en el párrafo 15 refiere que las intervenciones tendrán que ajustarse a los requisitos y límites previstos en la ley, así como que aquéllas que se realicen sin el cumplimiento de lo establecido carecerán de todo valor probatorio.

Lo mismo se refiere en la tesis P. XXXI/2008 emitida por el pleno de la Suprema Corte de Justicia de la Nación (SCJN), que señala que existe una imposibilidad constitucional para otorgar valor probatorio a las grabaciones derivadas de las intervenciones de comunicaciones privadas obtenidas sin autorización judicial.[5] De igual forma, se encuentra la tesis número P. XXXIII/2008, según la cual la intervención de comunicaciones privadas sin autorización judicial constituye prueba ilícita por mandato del artículo 16 constitucional, por lo que carece de todo valor probatorio.[6]

---

[5] Suprema Corte de Justicia de la Nación, *P. XXXI/2008*, México, novena época, pleno de la Suprema Corte de Justicia de la Nación: publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XXVII, Abril de 2008, página 5, dirección URL: https://sjf2.scjn.gob.mx/detalle/tesis/169884 [consulta: octubre, 2023].

[6] Suprema Corte de Justicia de la Nación, *P. XXXIII/2008*, México, novena época, pleno de la Suprema Corte de Justicia de la Nación: publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XXVII, Abril de 2008, página 6, dirección URL: https://sjf2.scjn.gob.mx/detalle/tesis/169859 [consulta: octubre, 2023].

Otra tesis relativa a la interpretación constitucional refiere que el derecho a la inviolabilidad de comunicaciones del artículo 16 de la CPEUM es oponible tanto a las autoridades como a los gobernados. Trasgredir esta prerrogativa implica incurrir en la comisión de un ilícito constitucional (Número de tesis: 2a. CLX/2000).[7]

Es importante destacar dos puntos de este artículo constitucional. Por un lado, se reconoce en el marco jurídico nacional la posibilidad de realizar estos actos excepcionales al derecho de la inviolabilidad de las comunicaciones privadas. Mientras que, por otro lado, establece la necesidad de un control constitucional por parte de los jueces de control a este tipo de actos de investigación realizados por el Ministerio Público.

Sin embargo, uno de los mayores vacíos legales es que la Carta Magna aborda exclusivamente las intervenciones relacionadas con el ámbito de procuración de justicia, no así por lo que hace a la seguridad pública y seguridad nacional que ni siquiera son enunciados.

1.1.2. Código Nacional de Procedimientos Penales (CNPP)[8]

El CNPP), al ser el ordenamiento adjetivo en materia procesal que aplica a nivel federal y en las 32 entidades federativas del país, aborda lo relacionado al ámbito de procuración de justicia. Lo relativo a las intervenciones se regula en el título V, sobre los “actos de investigación”, entre los artículos 291 y 303. Si bien no se hará una revisión pormenorizada de cada artículo, se delinearán algunas de las características principales.

El CNPP señala que será el titular de la FGR o de quienes éste delegue la facultad, así como de los titulares de las Fiscalías / Procuradurías locales, quienes podrán

[7] Suprema Corte de Justicia de la Nación, *2a. CLX/2000*, México, novena época, Segunda Sala de la Suprema Corte de Justicia de la Nación: publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XII, Diciembre de 2000, página 428, dirección URL: https://sjf2.scjn.gob.mx/detalle/tesis/190652 [consulta: octubre, 2023].

[8] Congreso de la Unión, *Código Nacional de Procedimientos Penales*, México, publicada en el Diario Oficial de la Federación el 05 de marzo de 2014, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf [consulta: julio, 2023].

solicitar al juez de control competente, por cualquier medio, la autorización para realizar la intervención expresando el objeto y la necesidad de la misma. El juez tendrá que resolver de manera inmediata sin que se excedan las seis horas posteriores a la recepción de la solicitud (artículo 291).

La solicitud debe estar fundada y motivada, además que debe de cumplir con una serie de características establecidas en la ley. Entre otros aspectos, debe de precisar la persona o personas sujetas a la medida, lugar o lugares donde se realizará, tipo de comunicación intervenida, duración, proceso que se llevará a cabo, números o aparatos, y denominación de las empresas de telecomunicaciones que la efectuarán. En el ámbito ministerial, las intervenciones no podrán exceder más allá de los seis meses (artículo 292).

El juez determinará las características de la intervención y podrá tener como objeto:

> *"…las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores…" (artículo 294).*

Las intervenciones tendrán que seguir los procedimientos específicos aprobados por el órgano judicial. En ese sentido, el juez podrá verificar que "las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total", por lo cual se requieren que el Ministerio Público responsable realice informes de cumplimiento que tendrá que enviar al juez de control (artículo 294).

De la misma forma, el policía de investigación o perito que coadyuvan en la investigación con el Ministerio Público, deben realizar un informe de resultados y un acta de conclusión cuando sea procedente (artículo 299).

Además, el órgano jurisdiccional ordenará la destrucción de los registros cuando se actualice alguna de las siguientes hipótesis: cuando no se relacione con los delitos investigados, cuando existan registros de información para los que no fue

autorizada, cuando rebasen los términos de la autorización, o cuando se decrete el archivo definitivo, el sobreseimiento o la absolución del imputado (artículo 300).

En este contexto, los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención (especialmente empresas telefónicas y de telecomunicaciones), deberán colaborar con la autoridad competente (artículo 301). A ellos se les podrá solicitar la información relativa a la localización geográfica en tiempo real o la entrega de datos conservados, información que tiene que ser proporcionada con la oportunidad y suficiencia necesaria a la autoridad investigadora (artículo 303). Tanto el concepto de "localización geográfica en tiempo real" como el de "datos conservados" se abordan específicamente en el capítulo 2.

Así, el CNPP en los artículos señalados integra aspectos fundamentales como el concepto de intervención de comunicaciones, la facultad del Ministerio Público de solicitar las intervenciones cuando estén relacionadas con un hecho con apariencia de delito, el control judicial, los informes de conocimiento, conclusión y destrucción de la información, así como la obligatoriedad de cooperación por parte de las empresas telefónicas y la introducción de los conceptos de localización geográfica en tiempo real y de entrega de datos conservados.

1.1.3. Ley Federal Contra la Delincuencia Organizada[9]

También en el ámbito de procuración de justicia se encuentra la Ley Federal Contra la Delincuencia Organizada, en la cual en diversos títulos se abordan las intervenciones de comunicaciones privadas. En el artículo 8, segundo párrafo, indica que la FGR contará con una unidad especializada que ejecutará los mandatos de la autoridad judicial para las intervenciones y verificará su autenticidad. De la misma manera, se señala que establecerá las características de los aparatos, equipos y sistemas a autorizar, así como la guarda, conservación, mantenimiento y

[9] Congreso de la Unión, *Ley Federal contra la Delincuencia Organizada*, México, publicada en el Diario Oficial de la Federación el 07 de noviembre de 1996, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFCDO.pdf [consulta: julio, 2023].

uso de los mismos. La información que obtenga esta unidad especializada podrá ser procesada y explotada para los fines de la investigación de delitos federales.[10]

El agente del Ministerio Público federal cuenta con una serie de actos reconocidos legalmente para la investigación, entre ellos, las intervenciones de comunicaciones privadas. Para su desahogo, la Fiscalía tendrá que emitir los protocolos que sean necesarios para el uso de este tipo de actos de investigación (Artículo 11 Bis 1).

De manera más concreta, se regulan en el Capítulo Sexto "De la Intervención de Comunicaciones Privadas", entre los artículos 16 y 28, tema que se abordará de manera particular en el "Capítulo 3. Análisis legal - institucional de las intervenciones de comunicaciones privadas utilizadas en dependencias de procuración de justicia, seguridad pública y seguridad nacional".

1.1.4. Ley de Guardia Nacional[11]

En lo relativo a la seguridad pública, el ordenamiento principal en la materia que es la Ley General del Sistema Nacional de Seguridad Pública, publicada en el Diario Oficial de la Federación (DOF) el 02 de enero de 2009, no hace referencia directa a la intervención de comunicaciones privadas.

Sin embargo, el tema se aborda en la Ley de Guardia Nacional, en el artículo 9, fracción XXVI, en el que se refiere que, con el fin de la prevención del delito, la dependencia puede solicitar al juez de control, en los términos del artículo 16 constitucional, la información de datos conservados y la georreferenciación de los

[10] En 2024, la Fiscalía Especializada en materia de Delincuencia Organizada (FEMDO) cuenta con la Unidad de Cuerpo Técnico de Control que "gestiona, ejecuta y registra los actos de investigación consistentes en la intervención de comunicaciones privadas en sus diversas modalidades, con autorización judicial, […] coordina la entrega de los registros y control de comunicaciones, y supervisa el uso y conservación de equipos, aparatos y sistemas asignados para el ejercicio de sus facultades". Vid. Fiscalía General de la República. *ACUERDO A/001/2023 por el que se emite el Manual de Organización y Procedimientos de la Fiscalía General de la República*, México, publicado en el Diario Oficial de la Federación el 09 de octubre de 2023, dirección URL: https://sidof.segob.gob.mx/notas/5704316 [consulta: noviembre, 2023].

[11] Congreso de la Unión, *Ley de la Guardia Nacional*, México, publicada en el Diario Oficial de la Federación el 27 de mayo de 2019, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf [consulta: julio, 2023].

equipos móviles de comunicación en tiempo real. Para esto, tiene que requerir los datos a los concesionarios, permisionarios, operadoras telefónicas y todas aquellas comercializadoras de servicios en materia de telecomunicaciones o de sistemas de comunicación vía satélite.

Antes de continuar, es preciso señalar que el artículo 21 de la CPEUM, sostiene que la GN es una institución policial federal que contribuye a la seguridad pública, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social. En el sector de seguridad pública federal, la GN es la encargada de realizar las intervenciones de comunicaciones previa autorización judicial.

En la Ley de la Guardia Nacional, esto se regula en el Título Séptimo “Controles”, Capítulo II “Del Control Judicial”, entre los artículos 100 y 106. Básicamente se establece que cuando existan indicios suficientes que acrediten que “se está organizando la comisión de delitos”, podrá realizar la solicitud el comandante o titular de la Jefatura General de Coordinación Policial de la institución, quien tendrá que dar vista al Ministerio Público en caso de que se actualice algún tipo de delito (artículo 100).

En el artículo 102 se indica que la solicitud, de manera similar a lo señalado en el CNPP, deberá contener los “preceptos legales que la fundamenten, el objeto y necesidad por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos, así como el periodo durante el cual se llevarán a cabo las intervenciones”. Y será la autoridad judicial quien, en su caso, aprobará y determinará las características específicas de la intervención.

Entre los delitos contemplados para la autorización de las intervenciones, sin ser exhaustivos, resaltan los siguientes en los términos del artículo 103:

- **Código Penal Federal**: evasión de presos; contra la salud; corrupción de menores e incapaces; pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprenderlo o resistirlo; turismo sexual en contra de personas menores de dieciocho años

de edad o de personas que no tienen capacidad para comprenderlo o resistirlo; explotación del cuerpo de un menor de edad por medio del comercio carnal; asalto en carreteras o caminos; homicidio relacionado con la delincuencia organizada; tráfico de menores; robo de vehículo; extorsión; y operaciones con recursos de procedencia ilícita.

- **Ley Federal de Armas de Fuego y Explosivos**: delito de introducción clandestina de armas de fuego.
- **Ley General de Salud**: delito de tráfico de órganos.
- **Ley de Migración**: delito de tráfico de indocumentados.
- **Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro:** delitos previstos en la ley.
- **Ley General en Materia de Desaparición Forzada de Personas, Desaparición cometida por Particulares, y del Sistema Nacional de Búsqueda de Personas**: delitos previstos en la ley.
- **Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas**: delitos previstos en la ley.

Refiere además que, cuando se requiera ampliar la intervención a otros sujetos o lugares, se deberá presentar una nueva solicitud. Al concluirse la intervención se debe levantar un acta con el inventario de audios, videos o imágenes captados. La GN pondrá a disposición del Ministerio Público el informe sobre la intervención (artículo 104).

En el caso que la autoridad judicial concluya que no hay elementos que pudieran constituir un delito, ordenará que se ponga a disposición la información resultado de las intervenciones, así como su destrucción en presencia del Comandante o Titular de la Jefatura General de Coordinación Policial de GN. En caso de no cumplirlo, podrá ser acreedor de sanciones penales, mientras que en el supuesto que efectivamente se tenga conocimiento de un delito se dará vista al Ministerio Público (artículo 105).

Por su parte, el artículo 106, señala que, para dar cumplimiento a las intervenciones autorizadas, el personal de GN deberá cumplir con tres requisitos: pertenecer a los

organismos de investigación o servicios técnicos especializados; contar con exámenes de control de confianza vigentes; y tener un grado mínimo de subinspector. Adicionalmente, deberá someterse a exámenes de control de confianza una vez concluida la intervención.

De esta forma, la Ley de la Guardia Nacional reconoce la investigación para la prevención de delitos federales, especialmente aquellos que están relacionados con el Código Penal Federal o los contenidos en leyes federales o generales.

1.1.5. Ley de Seguridad Nacional[12]

La seguridad nacional, de acuerdo con el artículo 5 de la ley en la materia, son las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano. Entre otras, se encuentran la protección frente a riesgos y amenazas, la preservación de la independencia y soberanía nacionales; el mantenimiento de las partes integrantes de la federación; la defensa legítima del Estados mexicano frente a otros Estados; así como la preservación de la democracia, fundada en el desarrollo social y político.

En este contexto, la Ley de Seguridad Nacional regula el tema en el Título Tercero “De la Inteligencia para la Seguridad Nacional”, Capítulo II “De las Intervenciones de Comunicaciones”, entre los artículos 33 y 49, donde se aborda la solicitud, procedimiento, vigencia de la autorización, obligaciones y casos de urgencia.

Al igual que en lo reconocido en el CNPP y en la Ley de la Guardia Nacional, es necesario que el CNI, que es la institución especializada, solicite a la autoridad judicial las intervenciones de comunicaciones privadas en materia de seguridad nacional (artículo 34).

No obstante, este ordenamiento jurídico establece la imposibilidad de que se realicen las intervenciones cuando estén fuera de los supuesto enunciados en el

[12] Congreso de la Unión, *Ley de Seguridad Nacional*, México, publicada en el Diario Oficial de la Federación el 31 de enero de 2005, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf [consulta: julio, 2023].

artículo 5 sobre las amenazas a la seguridad nacional. Asimismo, señala que será el Poder Judicial de la Federación (PJF) quien deberá conocer las solicitudes presentadas por el CNI (artículo 35).

Una de las principales diferencias con el CNPP y la LGN, es que las solicitudes no tendrán una naturaleza contenciosa y su funcionamiento carecerá de valor probatorio en procedimientos judiciales o administrativos (artículo 36). En otras palabras, las intervenciones tienen una naturaleza para realizar acciones de inteligencia o las actividades operativas que requiera la institución.

Las solicitudes que formule el CNI deberán contener una descripción de los riesgos o amenazas en términos del artículo 5, con identificación de datos específicos, mismos que serán presentados en sobre cerrado; las consideraciones que motivan la solicitud; y la vigencia de la autorización (artículo 38).

El juez debe emitir una resolución fundada y motivada sobre la autorización o la negativa (artículo 39). En la resolución se debe de considerar los datos del expediente, el lapso temporal y la autorización para instalar o remover instrumentos para realizar la intervención (artículo 40).

Los datos que se obtengan únicamente pueden ser conocidos por el Director General del CNI, las personas que designe el Consejo Nacional de Seguridad y los jueces federales competentes (artículo 41).

Sobre las obligaciones de los involucrados, el personal que realice las intervenciones debe mantener en secreto lo resultante de las intervenciones (artículo 45) y no podrá mantener el original o copias de la información (artículo 47); mientras que las empresas de telecomunicaciones deben dar todas las facilidades para la realización de las mismas (artículo 46).

En casos de excepción, cuando existan indicios de la existencia de una amenaza inminente a la seguridad nacional y cuando el procedimiento estándar entorpezca la investigación, el juez podrá autorizar de inmediato la solicitud (artículo 49).

En concreto, la Ley de Seguridad Nacional reconoce la investigación, con fines de inteligencia, de aquellas amenazas que puedan atentar contra el Estado mexicano, con la finalidad de prevenirlas o atenderlas.

1.1.6. Código Militar de Procedimientos Penales[13]

Igualmente en el ámbito de la seguridad nacional, se encuentra el Código Militar de Procedimientos Penales, que tiene aplicabilidad a la acción del personal adscrito a la Secretaría de la Defensa Nacional (SEDENA) y a la Secretaría de Marina – Armada de México (SEMAR), en cuanto al derecho penal dentro del fuero militar. Este ordenamiento regula lo relativo a las intervenciones entre los artículos 287 a 299.

Cabe mencionar que las intervenciones que incluye este Código es únicamente respecto de hechos que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia castrense. Es decir, el ordenamiento no regula su uso para la investigación de delitos del fuero civil desde el ámbito militar, esto es fundamental dado que no está normada su acción en el ámbito civil.

En la jurisdicción castrense, es el titular de la Fiscalía General de Justicia Militar o el servidor público a quien delegue esta facultad, quien puede realizar la solicitud de las intervenciones. La solicitud debe ser resuelta por el juez de control de manera inmediata en un plazo no mayor a las seis horas siguientes a que las haya recibido (artículo 287).[14]

Ésta debe estar debidamente fundada y motivada, además de cumplir una serie de características establecidas por la ley como precisar la persona o personas sujetas a la medida, identificación del lugar o lugares donde se realizará, el tipo de

[13] Congreso de la Unión, *Código Militar de Procedimientos Penales*, México, publicada en el Diario Oficial de la Federación el 16 de mayo de 2016, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/CMPP.pdf [consulta: julio, 2023].
[14] Cabe resaltar que el *Código Militar de Procedimientos Penales* señala que se podrá realizar la solicitud al "juez federal de control competente", por lo que se desprende que se realiza ante el Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones, y no frente al Juez Militar de Control.

comunicación intervenida, la duración, el proceso que se llevará a cabo y la empresa que la realizará (artículo 288).

Los objetos de la intervención pueden ser comunicaciones privadas orales, escritas, "por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma" (artículo 290).

El registro para las intervenciones debe garantizar que no se altere la fidelidad, autenticidad y contenido para que pueda ser ofrecida como medio de prueba en el proceso penal (artículo 293). Asimismo, deberá tener fecha de inicio y término, un inventario pormenorizado de documentos, objetos, sonidos o imágenes, así como otros datos que se consideren relevantes (artículo 294).

En suma, los ordenamientos jurídicos señalados hasta ahora son la base de la tesina en la medida en que son los cimientos normativos relacionados con las intervenciones de comunicaciones privadas en lo referente a procuración de justicia, seguridad pública y seguridad nacional. Sin embargo, el enramado normativo es más amplio y abarca otros instrumentos, como se verá a continuación.

1.1.7. Ley Orgánica del Poder Judicial de la Federación[15]

La Ley Orgánica del Poder Judicial de la Federación establece en el artículo 51, fracción III, que los jueces penales federales conocerán de las autorizaciones para intervenir cualquier comunicación, privada, así como la localización geográfica en tiempo real y la entrega de datos conservados.

De acuerdo con esta ley, se podrán intervenir comunicaciones según lo señalado en los siguientes ordenamientos jurídicos (artículo 52):

- Código Nacional de Procedimientos Penales;

[15] Congreso de la Unión, *Ley Orgánica del Poder Judicial de la Federación*, México, publicada en el Diario Oficial de la Federación el 07 de junio de 2021, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LOPJF.pdf [consulta: agosto, 2023].

- Ley de la Guardia Nacional;
- Ley de Seguridad Nacional;
- Ley Federal Contra la Delincuencia Organizada;
- Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro, Reglamentaria de la fracción XXI del artículo 73 de la CPEUM;
- Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos.

En el artículo 53, se establece también la posibilidad de incluir en las solicitudes todos aquellos delitos que ameriten prisión preventiva oficiosa de acuerdo con lo reconocido en el artículo 19 de la CPEUM.[16]

1.1.8. Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones

El Poder Judicial de la Federación, por conducto del Consejo de la Judicatura Federal, ha emitido diversos Acuerdos que instauran y regulan el funcionamiento del Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones (en adelante, Centro Nacional). El primero de ellos es el Acuerdo General 3/2017 que crea y establece el funcionamiento de este órgano, el cual comenzó a realizar funciones en mayo de 2017. Se compone por seis Jueces de Control y un Tribunal Unitario de Circuito que está habilitado como tribunal de alzada. Este Centro Nacional es competente para

[16] En el segundo párrafo del artículo 19 de la CPEUM, se enuncia el listado de delitos relacionados como son: "…abuso o violencia sexual contra menores, delincuencia organizada, homicidio doloso, feminicidio, violación, secuestro, trata de personas, robo de casa habitación, uso de programas sociales con fines electorales, corrupción tratándose de los delitos de enriquecimiento ilícito y ejercicio abusivo de funciones, robo al transporte de carga en cualquiera de sus modalidades, delitos en materia de hidrocarburos, petrolíferos o petroquímicos, delitos en materia de desaparición forzada de personas y desaparición cometida por particulares, delitos cometidos con medios violentos como armas y explosivos, delitos en materia de armas de fuego y explosivos de uso exclusivo del Ejército, la Armada y la Fuerza Aérea, así como los delitos graves que determine la ley en contra de la seguridad de la nación, el libre desarrollo de la personalidad, y de la salud".

conocer de la autorización de las intervenciones de comunicaciones privadas en todo el país.[17]

Prácticamente, desde 2017, todas las solicitudes en materia de intervenciones están centralizadas en este Centro Nacional, por lo que es sumamente relevante su función y es el órgano especializado del Poder Judicial de la Federación.

En el Acuerdo en comento se indica claramente que puede conocer de las solicitudes realizadas por el Ministerio Público Federal y de los titulares de los Ministerios Públicos locales, así como de aquellas realizadas por la GN y el CNI.

En el Acuerdo General 5/2019 señala que el Centro Nacional conocerá de las peticiones de localización geográfica en tiempo real o la entrega de datos conservados de los concesionarios de telecomunicaciones, tanto de las solicitudes como de las ratificaciones.[18] Por su parte, el Acuerdo General 12/2021 hace reformas relacionadas con periodos vacacionales, jornadas laborales y descansos del personal adscrito a este Centro Nacional.[19]

---

[17] Consejo de la Judicatura Federal, *Acuerdo General 3/2017 del Pleno del Consejo de la Judicatura Federal, por el que se crea el Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones*, publicado en el Diario Oficial de la Federación el 15 de mayo de 2017, dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5482579&fecha=15/05/2017#gsc.tab=0 [consulta: agosto, 2023].

[18] Consejo de la Judicatura Federal, *Acuerdo General 5/2019 del Pleno del Consejo de la Judicatura Federal, que reforma los artículos 14 y 19 del Diverso 3/2017, por el que se crea el Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones*, publicado en el Diario Oficial de la Federación el 21 de mayo de 2019, dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5560782&fecha=21/05/2019#gsc.tab=0 [consulta: agosto, 2023].

[19] Consejo de la Judicatura Federal, *Acuerdo General 12/2021, del Pleno del Consejo de la Judicatura Federal, que Reforma el Artículo 13, del similar 3/2017 del Pleno del Consejo de la Judicatura Federal por el que se Crea el Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones; en Relación con su Periodo Vacacional*, publicado el 20 de septiembre de 2021, dirección URL: https://www.google.com/search?q=ACUERDO+GENERAL+12%2F2021%2C+DEL+PLENO+DEL+CONSEJO+DE+LA+JUDICATURA+FEDERAL%2C+QUE+REFORMA+EL+ART%C3%8DCULO+13%2C+DEL+SIMILAR+3%2F2017+DEL+PLENO+DEL+CONSEJO+DE+LA+JUDICATURA+FEDERAL+POR+EL+QUE+SE+CREA+EL+CENTRO+NACIONAL+DE+JUSTICIA+ESPECIALIZADO+EN+CONTROL+DE+T%C3%89CNICAS+DE+INVESTIGACI%C3%93N%2C+ARRAIGO+E+INTERVENCI%C3%93N+DE+COMUNICACIONES%3B+EN+RELACI%C3%93N+CON+SU+PERIODO+VACACIONAL.&oq=ACUERDO+GENERAL+12%2F2021%2C+DEL+PLENO+DEL+CONSEJO+DE+LA+JUDICATURA+FEDERAL%2C+QUE+REFORMA+EL+ART%C3%8DCULO+13%2C+DEL+SIMILAR+3%2F2017+DEL+PLENO+DEL+CONSEJO+DE+LA+JUDICATURA+FEDERAL+POR+EL+Q

En suma, es el órgano donde confluyen las solicitudes realizadas en todo el país, por lo que cuenta con jueces de control especializados quienes son los responsables de autorizar o negar las solicitudes de las instituciones ya referidas.

1.1.9. Código Penal Federal[20]

El Código Penal Federal refiere las sanciones relacionadas con delitos de intervenciones de comunicaciones. En ese sentido, a quien intervenga comunicaciones sin mandato de autoridad competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días de multa (artículo 177).

A la persona física o representante de la persona moral requerida por el Ministerio Público, que rehusare a aportar información de intervenciones en tiempo real o que obstaculice o retrase sin causa justificable, se le impondrá una prisión de tres a ocho años y de cinco mil a diez mil días de multa (artículo 178 Bis).

Asimismo, a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas por intervenciones, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa (artículo 211 Bis).

1.2. Instrumentos jurídicos internacionales

Si bien existe un marco jurídico que tiene aplicabilidad nacional, paralelamente existen una serie de instrumentos jurídicos propios del derecho internacional público

UE+SE+CREA+EL+CENTRO+NACIONAL+DE+JUSTICIA+ESPECIALIZADO+EN+CONTROL+DE+T%C3%89CNICAS+DE+INVESTIGACI%C3%93N%2C+ARRAIGO+E+INTERVENCI%C3%93N+DE+COMUNICACIONES%3B+EN+RELACI%C3%93N+CON+SU+PERIODO+VACACIONAL.&aqs=chrome..69i57.598j0j7&sourceid=chrome&ie=UTF-8 [consulta: agosto, 2023].

[20] Congreso de la Unión, *Código Penal Federal*, México, publicada en el Diario Oficial de la Federación el 14 de agosto de 1931, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf [consulta: mayo, 2023].

que abordan indirectamente, de manera tangencial o por interpretación las intervenciones de comunicaciones privadas.

Destaca el hecho que no se identificó un ordenamiento supranacional vinculante para México que aborde de manera específica el tema de las intervenciones de comunicaciones privadas. A continuación, se presentan los principales hallazgos resultantes de la búsqueda realizada.

1.2.1. Declaración Universal de Derechos Humanos (1948)

La Declaración Universal de los Derechos Humanos, proclamada el 10 de diciembre de 1948, establece en el artículo 12 el derecho a la privacidad y a la protección contra ataques a la honra y la reputación. Señala que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación”.[21]

Este derecho debe estar garantizado respecto a las posibles injerencias o ataques provenientes de autoridades gubernamentales, de personas morales o personas físicas. Como lo establece la Corte Interamericana de Derechos Humanos “las autoridades competentes sólo deben pedir aquella información relativa a la vida privada de las personas cuyo conocimiento resulte indispensable para los intereses de la sociedad”.[22]

1.2.2. Pacto Internacional de Derechos Civiles y Políticos (1976)

El 23 de marzo de 1976, entró en vigor el Pacto Internacional de Derechos Civiles y Políticos que, en el artículo 17, indica que “nadie será objeto de injerencias

[21] Asamblea General de las Naciones Unidas, *Declaración Universal de Derechos Humanos*, 10 de diciembre de 1948, dirección URL: https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf [consulta: septiembre, 2023].
[22] Gobierno de la República, *Declaración Universal. Versión Comentada*, Guatemala, 2011, dirección URL: https://www.corteidh.or.cr/tablas/28141.pdf [consulta: septiembre, 2023].

arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación".[23]

En ese orden de ideas, prohíbe la interferencia arbitraria en la vida privada, que incluye la protección de la correspondencia y se podría interpretar, en un sentido amplio, de las comunicaciones privadas. Además, señala que toda persona tendrá derecho a la protección de la ley contra cualquier tipo de injerencias o ataques.

1.2.3. Convención Americana sobre Derechos Humanos (1981)[24]

La Convención Americana sobre Derechos Humanos, también conocida como Pacto de San José de Costa Rica, fue publicada el 7 de mayo de 1981. Al igual que los instrumentos internacionales anteriores, no aborda directamente el tema de las intervenciones de comunicaciones privadas.

No obstante, en el artículo 11, relativo a la protección de la honra y la dignidad, establece principios muy similares al Pacto Internacional de Derechos Civiles y Políticos de la sección pasada, al referir que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación."

En los mismos términos, señala que las personas tienen derecho a la protección de la ley contra injerencias y ataques. En ese sentido, también al apegarse a la hermenéutica jurídica, se podría inferir, que incluye a las intervenciones de comunicaciones privadas.

[23]Asamblea General de las Naciones Unidas, Pacto Internacional de Derechos Civiles y Políticos, diciembre de 1996, dirección URL: https://www.ohchr.org/sites/default/files/ccpr_SP.pdf [consulta: septiembre, 2023].

[24] Organización de Estados Americanos, *Convención Americana Sobre Derechos Humanos*, mayo de 1991, dirección URL: https://www.cndh.org.mx/sites/default/files/doc/Programas/TrataPersonas/MarcoNormativoTrata/InsInternacionales/Regionales/Convencion_ADH.pdf [consulta: septiembre, 2023].

1.2.4. Convención Interamericana contra la Corrupción (1997)[25]

La Convención Interamericana contra la Corrupción, que entró en vigor en 1997, tiene como propósito promover, facilitar y regular la cooperación entre los Estados Parte a fin de prevenir, detectar, sancionar y erradicar los actos de corrupción en el ejercicio de las funciones públicas y los actos de corrupción específicamente vinculados con tal ejercicio.

Aunque tampoco es un instrumento directamente relacionado con las intervenciones de comunicaciones privadas, establece disposiciones relacionadas con la cooperación internacional en la lucha contra la corrupción, que podría tener implicaciones en la obtención y el intercambio de información, incluyendo este tipo de actos de investigación.

Dentro del instrumento se señala que se prestará la más amplia cooperación mutua sobre las formas y métodos para prevenir, detectar, investigar y sancionar los actos de corrupción. Se reconoce, entre otras medidas, la asistencia en la identificación, rastreo, inmovilización, confiscación y decomiso de bienes obtenidos o derivas de la comisión de los delitos o bienes utilizados en su comisión o producto de ésta.

1.2.5. Tratado Bilateral con Estados Unidos (1987)[26]

El *Tratado de Cooperación entre los Estados Unidos Mexicanos y los Estados Unidos de América sobre Asistencia Jurídica Mutua de 1987*, es el único instrumento internacional con el que se cuenta actualmente para el intercambio de información a nivel bilateral, al menos por lo que hace a procuración de justicia.

---

[25] Organización de Estados Americanos, *Convención Interamericana contra la Corrupción*, Venezuela, marzo de 1997, dirección URL: https://www.oas.org/es/sla/ddi/docs/tratados_multilaterales_interamericanos_b-58_contra_corrupcion.pdf [consulta: septiembre, 2023].

[26] Gobierno de México, *Tratado de Cooperación entre los Estados Unidos Mexicanos y los Estados Unidos de América sobre Asistencia Jurídica Mutua*, México, Ciudad de México, diciembre de 1987, dirección URL: https://aplicaciones.sre.gob.mx/tratados/ARCHIVOS/EUA-ASISTENCIA%20JURIDICA.pdf [consulta: septiembre, 2023].

De acuerdo con el artículo 1°, párrafo primero, la finalidad del tratado es que las partes cooperen entre sí tomando todas las medidas apropiadas que se puedan implementar legalmente a fin de prestarse asistencia jurídica mutua. Además, el Tratado contempla la prevención, la investigación, la persecución de delitos o cualquier otro procedimiento penal, que inicie por hechos que estén dentro de la competencia o jurisdicción de la Parte requirente cuando la asistencia sea solicitada.

Conforme al párrafo cuarto de este primer artículo, la asistencia incluirá el suministro de documentos, registros o declaraciones; la localización o identificación de personas; el intercambio de información; u otras formas de asistencia mutuamente convenidas entre las partes.

A su vez, el artículo 13, relativo a la localización o identificación de personas, establece que la Parte requerida adoptará "todas las medidas necesarias para localizar o identificar a las personas que se cree se encuentran en dicho Estado y que se necesitan en relación con una investigación, procedimiento o diligencia dentro del ámbito de aplicación del Tratado".

Aunque el instrumento bilateral en comento es del año 1987, es el que actualmente se utiliza para el intercambio de información y de intervenciones de comunicaciones privadas entre los países. Uno de los retos que tiene este Tratado es que, por la fecha en la que fue signado, no contempla los avances tecnológicos, como los dispositivos electrónicos que han surgido en las últimas décadas y las nuevas modalidades de intercambio de información y de comunicaciones.

1.2.6. Convención sobre Ciberdelincuencia del Consejo de Europa (2001)

Si bien no aplica al caso mexicano, el Consejo de Europa emitió el 23 de noviembre de 2001, el Convenio sobre la Ciberdelincuencia, también conocido como Convenio de Budapest, el cual es considerado como una buena práctica internacional.

Este convenio considera la "interceptación de telecomunicaciones" y la "vigilancia electrónica". En el artículo 3, describe el delito de "interceptación ilícita", el cual

corresponde a la violación de la privacidad de las comunicaciones a través de la intervención o grabación de medios como teléfono, fax, correo electrónico o transferencia de archivos. Este delito incluye:

> *"…escuchar, monitorear o vigilar el contenido de las comunicaciones, a adquirir los contenidos de datos, ya sea en forma directa, mediante el acceso y uso del sistema informático, o en forma indirecta, mediante el uso de dispositivos electrónicos para escuchar en forma secreta o de dispositivos para intervenir conversaciones. La interceptación puede implicar también la grabación…".*[27]

Incluye no sólo la información de las personas físicas, sino que también se integran empleados o actividades comerciales, sistemas informáticos, incluso emisiones radioeléctricas y electromagnéticas, *cookies* y otros aspectos, por lo que se contemplan aspectos que van más allá de los supuestos identificados por la legislación mexicana. Por ejemplo, considera las "emisiones electromagnéticas" que pueden ser emitidas por un ordenador durante su funcionamiento y posteriormente reconstruidas para identificar las comunicaciones que integran.

Más adelante, en el artículo 14, señala que la interceptación de llamadas debe de estar limitada a una serie de delitos graves. El artículo 20 reconoce la necesidad de obtener información en tiempo real para las investigaciones penales, mientras que el artículo 21 indica que por "datos relativos al contenido" se entiende como todo los transmitido como parte de las comunicaciones.

A diferencia del Tratado Bilateral con Estados Unidos referido en la sección anterior, esta Convención tiene una interpretación mucho más amplia y actualizada sobre el concepto de "comunicaciones" incluyendo los avances tecnológicos. Esto podría servir de precedente para los organismos supranacionales de la región y para el Estado mexicano.

[27] Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, Bruselas, noviembre de 2021, dirección URL: https://rm.coe.int/16802fa403 [consulta: septiembre, 2023].

1.3. Consideraciones finales del capítulo

Actualmente existe un marco jurídico importante sobre intervención de comunicaciones privadas a nivel federal que tiene aplicabilidad en los estados del país, el cual se desprende de la Carta Magna que reconoce el derecho humano a la inviolabilidad de las comunicaciones privadas. A partir de éste se configura un enramado jurídico muy importante que impacta los ámbitos de procuración de justicia, seguridad pública y seguridad nacional.

En procuración de justicia, el ordenamiento que regula lo relativo a la función de la FGR y las fiscalías de las 32 entidades federativas, es el CNPP. Establece los procedimientos específicos para la investigación y persecución del delito utilizando las intervenciones de comunicaciones privadas, así como su incorporación a las Carpetas de Investigación como dato y medio de prueba previa autorización del juez competente. Por su parte, la Ley Federal contra la Delincuencia Organizada reconoce una unidad especializada dentro de la FGR encargada de realizar las intervenciones, así como otra serie de acciones para la emisión de protocolos y la definición de las tecnologías que pueden ser utilizadas para implementarlas. Como se mencionó, las intervenciones en este ámbito tienen como finalidad la investigación y persecución del delito.

En lo relativo a seguridad pública, es la Ley de Guardia Nacional la que regula el tema. A diferencia del rubro anterior, no hace referencia a las policías de las entidades federativas, sino que únicamente tiene aplicabilidad al ámbito federal. Incorpora la posibilidad de que la GN realice las intervenciones de manera preventiva cuando se acredite que se está organizando la comisión de delitos en materia de armas, contra la salud, migración, secuestro, desaparición de personas, trata de personas y otros contenidos en el Código Penal Federal. Al igual que en procuración de justicia, requieren un control constitucional ejercido por los jueces adscritos al Centro Nacional. En este supuesto, las intervenciones buscan prevenir delitos federales de alto impacto.

Por lo que hace al rubro de seguridad nacional, es la ley en la materia que contiene un apartado específico para las intervenciones de comunicaciones privadas. De

acuerdo con la Ley de Seguridad Nacional, pueden ser aprobadas por el juez de control cuando sean útiles para prevenir o proteger al Estado Mexicano frente a los riesgos o amenazas contenidos en el artículo 5. Por mencionar algunos supuestos reconocidos, se encuentran la preservación de la independencia y soberanía nacionales; el mantenimiento de las partes integrantes de la federación; la defensa legítima del Estado mexicano frente a otros Estados; así como la preservación de la democracia, fundada en el desarrollo social y político. En ese sentido, se podrían considerar como intervenciones en materia de inteligencia para la prevención de riesgos y amenazas contra el Estado Mexicano. Por su parte, las Fuerzas Armadas carecen de un marco jurídico en el fuero civil.

En cuanto al ámbito internacional, los instrumentos jurídicos identificados y citados en el apartado no abordan directamente las intervenciones de comunicaciones privadas. Todos ellos hacen referencia al derecho a la privacidad o la prohibición a la interferencia arbitraria de la vida privada. El Pacto Internacional de Derechos Civiles y Políticos refiere el tema de la correspondencia, lo cual podría interpretarse como parte de las comunicaciones privadas, aunque es un tema demasiado puntual.

Con Estados Unidos, existe el *Tratado de Cooperación entre los Estados Unidos Mexicanos y los Estados Unidos de América sobre Asistencia Jurídica Mutua de 1987*, el cual es utilizado actualmente para el intercambio de información en el ámbito de procuración de justicia y tiene aplicabilidad a las intervenciones.

Por su relevancia, si bien no aplica al caso mexicano, se aborda brevemente la *Convención sobre Ciberdelincuencia del Consejo de Europa* que es uno de los instrumentos más importantes en la materia a nivel internacional. Regula la “intercepción ilícita”, además de una serie de supuestos importantes como la información derivada de actividades comerciales, sistemas informáticos, emisiones radioeléctricas y electromagnéticas, entre otros.

Actualmente no se cuenta con un ordenamiento internacional especializado en la materia que sea aplicable para el caso mexicano. Lo anterior puede ser considerado como un vacío normativo dado que es necesario regular a nivel regional e

internacional, especialmente por la importancia creciente de las intervenciones en las investigaciones penales en un contexto donde existe un aumento importante de las tecnologías de la información y de la comunicación.

Capítulo 2. Definición y modalidades de las intervenciones de comunicaciones privadas

En este segundo capítulo se analiza la definición, las modalidades y los responsables de proveer la información relacionada con las intervenciones de comunicaciones privadas de acuerdo con la normatividad mexicana. Asimismo, se aborda brevemente las características de una nueva modalidad que podría ser incluida explícitamente en el marco jurídico en la materia.

2.1. Definición de intervención de comunicaciones privadas

En la legislación mexicana se identificaron cuatro definiciones sobre intervención de comunicaciones privadas, mismas que se presentan y se discuten en esta sección. El primer concepto se encuentra en la Ley Federal contra la Delincuencia Organizada, específicamente en el artículo 16, donde lo refiere de la siguiente manera:

> *"…La intervención de comunicaciones privadas, abarca todo un sistema de comunicación, o programas que sean fruto 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, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo…".* [28]

Al ser publicada esta ley en 1996, es la primera definición identificada en el marco jurídico mexicano y establece los elementos que retomarán otros conceptos incluidos posteriormente en la legislación nacional.

En un segundo término, la Ley de Seguridad Nacional de 2005, en su artículo 34, segundo párrafo, la refiere como:

[28] Congreso de la Unión, *Ley Federal contra la Delincuencia Organizada*, *Óp. Cit*., artículo 16.

"…Se entiende por intervención de comunicaciones la toma, escucha, monitoreo, grabación o registro, que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología…".[29]

Varios años más tarde, en 2014, el Código Nacional de Procedimientos Penales, en el artículo 291, segundo párrafo, el cual fue reformado en junio de 2016, puntualiza el siguiente término:

"…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…".[30]

Posteriormente, el Código Militar de Procedimientos Penales (2016), en el artículo 287, segundo párrafo, dice a la letra:

"…La intervención de comunicaciones privadas, abarca todo un sistema de comunicación, o programas que sean fruto 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, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo…".[31]

Es necesario puntualizar, como se mencionó en el capítulo anterior, que las intervenciones que reconoce este Código Militar son únicamente respecto de hechos constitutivos de delito que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia castrense.

Así, a lo largo de prácticamente dos décadas del desarrollo legal del concepto, estas definiciones tienen cuando menos cuatro puntos en común que es necesario rescatar:

[29] Congreso de la Unión, *Ley de Seguridad Nacional*, *Óp. Cit*., artículo 34.
[30] Congreso de la Unión, *Código Nacional de Procedimientos Penales*, *Óp. Cit*., artículo 291.
[31] Congreso de la Unión, *Código Militar de Procedimientos Penales*, *Óp. Cit*., artículo 287.

- **Tipo de medio**. Al “abarcar todo sistema de comunicación o programas que sean frutos de la evolución tecnológica” o “por cualquier medio, aparato o tecnología”, el legislador previó la posibilidad del avance en los medios y formas de comunicación, por lo que contempla cualquier dispositivo o tecnología nueva, incluyendo plataformas de internet, aplicaciones telefónicas u otras similares. Sin embargo, como se sostiene más adelante, es posible que sea una definición laxa en lo relativo al avance tecnológico que requiere una mayor puntualización.
- **Tipo de comunicación.** También contempla el “intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos”, con lo cual se puede abarcar una gran cantidad de supuestos que van, desde comunicaciones escritas hasta mensajes electrónicos, así como comunicaciones orales, por medios videográficos, ubicaciones, o cualquier otro tipo de archivo que pueda ser intercambiado.
- **Tipo de acción.** Cuando se refiere a la “toma, escucha, monitoreo, grabación o registro”, evoca los verbos rectores o acciones que pueden realizar las instituciones de gobierno en materia de intervención de comunicaciones, previa autorización de la autoridad judicial competente. Estos supuestos son el sustento de las modalidades de intervenciones que se abordan más adelante en este capítulo.
- **Temporalidad.** Al referirse a que las intervenciones pueden ser “en tiempo real o con posterioridad”, abre la posibilidad a que puedan realizarse prácticamente en cualquier momento que las autoridades lo requieran. Esto brinda un amplio margen de acción institucional.

Si bien los elementos que reconocen estos ordenamientos son adecuados y contemplan muchos de los supuestos en los que podrían realizarse las intervenciones, es necesario destacar que no existe una definición única, que sea aplicable a todos los escenarios.

2.2. Modalidades de intervenciones de comunicaciones privadas reconocidas legalmente

Legalmente están definidas y cuentan con características señaladas explícitamente en la ley cuatro modalidades de intervención de comunicaciones: datos conservados, localización geográfica en tiempo real, extracción de información de dispositivos electrónicos y escuchas. Estas modalidades están reconocidas principalmente en la Ley Federal de Telecomunicaciones y Radiodifusión[32] y en los Lineamientos de Colaboración en Materia de Seguridad y Justicia[33] (en adelante, Lineamientos) del Instituto Federal de Telecomunicaciones (IFETEL). Al final del apartado se hace una breve reflexión sobre otras modalidades que, por sus características, también podrían ser incluidas como clasificaciones particulares.

2.1.1. Datos conservados

De acuerdo con la Ley Federal de Telecomunicaciones y Radiodifusión, artículo 190, fracción II, las empresas de telecomunicaciones[34] deben conservar un registro y control de las comunicaciones que se realicen desde cualquier tipo de línea propia o arrendada, bajo cualquier modalidad, que permita identificar los siguientes datos:

- Nombre, denominación o razón social y domicilio del suscriptor.
- Tipo de comunicación (transmisión de voz, buzón vocal, datos), servicios suplementarios (reenvío o transferencia de llamada) o servicios de

[32] Congreso de la Unión, *Ley Federal de Telecomunicaciones y Radiodifusión*, México, publicada en el Diario Oficial de la Federación el 14 de julio de 2014, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf [consulta: octubre de 2023].

[33] Instituto Federal de Telecomunicaciones, *Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996*, México, publicada en el Diario Oficial de la Federación, el 02 de diciembre de 2015, dirección URL: https://dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015&print=true [consulta: octubre de 2023].

[34] Cuando se habla de "empresas de telecomunicaciones" se hace referencia a dos categorías particulares: 1) Concesionarios: es persona física o moral, titular de una concesión única o de red pública de telecomunicaciones que les permite prestar servicios públicos de telecomunicaciones; y 2) Autorizados: son aquellos que cuenten con título habilitante para establecer y operar o explotar una comercializadora de servicios de telecomunicaciones sin tener el carácter de Concesionario, o para explotar los derechos de emisión y recepción de señales de satélites extranjeros que cubran y puedan prestar servicios en el territorio nacional. *Vid*. Congreso de la Unión, *Ley Federal de Telecomunicaciones y Radiodifusión*, *Óp. Cit.*, artículo segundo, fracción IIV y VIII.

mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados).

- Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil, modalidad de líneas con trato o plan tarifario, como líneas de prepago.
- Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia.
- Fecha y hora de la primera activación del servicio y la etiqueta de localización.
- Identificación y características técnicas de los dispositivos.
- Ubicación digital del posicionamiento geográfico de las líneas telefónicas.

Complementariamente a lo anterior, en los Lineamientos, en el artículo décimo cuarto, se establece que para líneas privadas se registrará el usuario, la dirección de origen y destino de la línea.

Del servicio fijo se conservará la siguiente información:

- Nombre y dirección del usuario registrado.
- Tipo de comunicación.
- Números de origen y destino.
- Duración, fecha y hora de la comunicación.

En lo relativo al servicio móvil en las modalidades de prepago y pospago:

- Nombre y dirección del usuario registrado, en el caso de la modalidad de pospago.
- Tipo de comunicación.
- Los números de origen y destino.
- Duración, fecha y hora de la comunicación.
- Fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda).
- La etiqueta de localización (identificador de celda).

- IMEI.[35]
- IMSI.[36]
- En su caso, los IMSIs asociados a un mismo IMEI.
- Modalidad de pago, y
- En su caso, características técnicas del Dispositivo o Equipo Terminal Móvil.[37]

En caso de modalidad de prepago:

- El lugar, fecha y hora en la que se realizó la compra del dispositivo de prepago y/o la tarjeta SIM, en el caso en que el Concesionario o Autorizado los comercialice por canales propios, o
- En su caso, los datos del distribuidor al que fue entregado el dispositivo de prepago o la tarjeta SIM para su comercialización.

Los datos conservados permiten obtener información clave relacionada con identificación del titular de la línea, ubicaciones aproximadas[38] de personas a lo largo de meses, reconstrucción de rutas de movilidad, identificación de las redes de comunicación, historial de llamadas realizadas, duración de éstas, números de teléfono asociados a determinados equipos celulares, tipos de comunicación, entre otros aspectos. Por lo tanto, la información proveniente de datos conservados es fundamental para las investigaciones que se puedan realizar en procuración de justicia, seguridad pública y/o seguridad nacional.

---

[35] Es el código de identidad de fabricación del equipo (*International Mobile Equipment Identity number*, por sus siglas en inglés). *Vid*. Instituto Federal de Telecomunicaciones, *Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996*, *Óp. Cit*., artículo segundo, fracción XIV.

[36] Es la identidad internacional de suscripción al servicio móvil conforme al Plan de identificación internacional para redes públicas y suscripciones; o código de identidad internacional del usuario móvil (*International Mobile Subscriber Identity*, por sus siglas en inglés). *Vid*. *Ídem*, artículo segundo, fracción XV.

[37] Es el equipo que utiliza el usuario para conectarse más allá del punto de conexión terminal de una red pública con el propósito de tener acceso y/o recibir uno o más servicios de telecomunicaciones móviles. *Vid*. *Ídem*, artículo segundo, fracción XI.

[38] Se señala que aporta la “ubicación aproximada” dado que se comparte la información de la ubicación de la antena más próxima a la que está conectado el dispositivo electrónico.

2.1.2.Localización geográfica en tiempo real

Los Lineamientos en el artículo cuarto se señalan los requerimientos de localización geográfica en tiempo real de los dispositivos o teléfonos celulares, los cuales deberán contener la siguiente información (mucha de la cual comparten con los datos conservados):[39]

- Fecha y lugar.
- Nombre y cargo del servidor público requirente e institución a la que pertenece.
- Fecha en que se publicó en el DOF la designación de la Autoridad.
- Fundamento legal del requerimiento.
- Número(s) telefónico(s) a diez dígitos, IMSI o IMEI objeto del requerimiento.
- Objeto de la solicitud:
    - Localización geográfica en tiempo real.
    - Entrega de datos conservados.
- Periodo por el que se solicita la información.
- Formatos en el que se requiere sea entregada la información (por ejemplo, "pdf", ".xls" o ".csv").
- Sello de la Institución, y
- Firma autógrafa o electrónica del servidor público designado.

De acuerdo con el ordenamiento referido se dará prioridad a las solicitudes que se refieran a situaciones donde se encuentre en peligro la vida de una o más personas, o cuando se actualice alguna de las amenazas a la seguridad nacional referida en la ley en la materia.

Asimismo, se mantendrá el alcance temporal que especifique el requerimiento pudiendo ser reconfigurada la frecuencia con la que se actualice la información de

[39] Instituto Federal de Telecomunicaciones, *Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996*, *Óp. Cit*.

localización geográfica, por ejemplo, en horas, minutos o en tiempo real (Lineamientos, artículo noveno).

Por su parte, la localización geográfica en tiempo real, como su nombre lo indica, aporta la ubicación aproximada[40] de un equipo de telecomunicaciones asociado con una persona al momento, por lo que es útil cuando menos para tres propósitos: 1) para identificar víctimas en situaciones en los que un delito se está cometiendo (como secuestro o desaparición de personas); 2) para dar seguimiento a potenciales infractores de la ley que se están desplazando, para la ejecución de una orden de cateo o una orden de aprehensión; y 3) para la toma de decisiones por parte de las autoridades con la finalidad de realizar acciones operativas al desplazar personal o evitar posibles riesgos.

2.1.3.Extracción de información de dispositivos electrónicos

Se identificaron dos definiciones específicas sobre la extracción de información de dispositivos electrónicos. La primera se ubica en el CNPP, en el artículo 291, párrafo cuarto, el cual fue reformado el 17 de junio de 2016, que establece lo siguiente:[41]

> *"… [La extracción de información] 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…".*

La segunda definición se reconoce en el Código Militar de Procedimientos Penales, en el artículo 187, tercer párrafo, el cual dice a la letra:[42]

> *"… [La extracción de información] consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos,*

[40] Al igual que en datos conservados, se señala que aporta la "ubicación aproximada" dado que se comparte la información de la ubicación de la antena más próxima a la que está conectado el dispositivo electrónico.
[41] Congreso de la Unión, *Código Nacional de Procedimientos Penales*, *Óp. Cit*.
[42] Congreso de la Unión, *Código Militar de Procedimientos Penales*, *Óp. Cit*.

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…"

Los conceptos enunciados con anterioridad, salvo por mínimas diferencias, prácticamente contienen los mismos elementos. Hacen referencia a la actividad que realiza la institución para obtener datos de texto, audio, imagen o video de cualquier dispositivo tecnológico que pueden ser traducidos como teléfonos celulares, laptops, computadoras de escritorio, discos duros, USB, drones, radios matra, entre otros.

2.1.4.Escuchas

A diferencia de las modalidades anteriores que tienen una definición clara establecida en las leyes, códigos o lineamientos aplicables, lo relativo a las escuchas no cuenta con un concepto específico brindado en el marco legal. En todo caso, se deprende de la interpretación de los cuatro conceptos dados en el primer apartado del presente capítulo relativo a la conceptualización de las intervenciones de comunicaciones privadas.

Si bien la intención del subapartado no es retomar las definiciones que ya se abordaron, sí es necesario referir algunos aspectos específicos. Los conceptos ya enunciados refieren, con ciertos matices, que las escuchas consisten en el monitoreo, grabación, registro o conservación de contenido sobre conversaciones entre dos o más personas que se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo, por cualquier medio, aparato o tecnología.

Las escuchas son fundamentales para los ámbitos de procuración de justicia, seguridad pública y seguridad nacional debido a que permiten obtener datos que se desprendan de las comunicaciones entre dos o más personas para la prevención, investigación y persecución de delitos, como pueden ser nombres, lugares potencialmente asociados con delitos, organización de hechos delictivos, posibles

cómplices, redes criminales, identificación de víctimas, zonas de operación, vehículos u otros objetos asociados con la comisión de ilícitos, etc.

Sin embargo, sería importante, al igual que con las otras modalidades, contar con una definición particular, ya que la situación actual puede prestarse a la potencial realización de actos arbitrarios.

2.1.5.Otras categorías

Las cuatro modalidades anteriores son las que “tradicionalmente” han sido utilizadas por las instituciones de procuración de justicia, seguridad pública y seguridad nacional. No obstante, producto del proceso de evolución tecnológica y de los avances en términos de telecomunicaciones sería posible delinear o incorporar de manera explícita otra u otras modalidades con las siguientes características:

- **Mensajería, llamadas, videollamadas u otras comunicaciones por internet**. En los últimos años, las formas de comunicación han migrado de llamadas analógicas, es decir, comunicaciones realizadas de un equipo de teléfono celular o línea fija a otra similar, hacia comunicaciones a través de internet, tanto mensajes como llamadas, videollamadas y otras formas de comunicación (por ejemplo, emoticones). En estos procesos actuales, ha sido fundamental el surgimiento de aplicaciones como *Facebook, Instagram, WhatsApp, Telegram, Signal, Confide, Twitter* (ahora “X”), etc., que contienen una gran cantidad de información entre las personas involucradas en el proceso comunicativo que puede ser útil potencialmente para una investigación. Esto tiene debería ser reconocido explícitamente en el marco legal.
- **Aplicaciones tecnológicas, buscadores y/o páginas de internet**. Aunque en la misma línea, existen otras plataformas, aplicaciones tecnológicas, buscadores o páginas de internet que también contienen información específica. En esta categoría se podrían encontrar algunas como *Google,*

Uber, Didi, Indrive, Tinder, Netflix y algunas otras plataformas., las cuales podrían contener y aportar datos relevantes para investigaciones en materia de procuración de justicia y seguridad, en los términos referidos en esta tesina.

Habitualmente las compañías propietarias de estas plataformas son extranjeras y actúan con base en políticas propias, y no necesariamente a partir de la legislación nacional. Es necesario reforzar el marco jurídico en la materia para hacerlo vinculante. Lo anterior tendría que implicar su inclusión en la legislación a partir del proceso legislativo.

Las modalidades señaladas anteriormente deben de aportar, de manera ágil y a partir de procesos prestablecidos, información de utilidad para identificar presuntos hechos delictivos antes de que sean cometidos; para aportar datos fehacientes que puedan relacionar a un presunto responsable con un hecho presumiblemente constitutivo de delito; o para prevenir o realizar acciones para la contención de amenazas a la seguridad nacional.

2.3. Responsables de entrega de información[43]

De acuerdo con los Lineamientos, las autoridades facultadas son las instancias de seguridad, procuración de justicia y administración de justicia que, “conforme a sus atribuciones previstas en sus leyes aplicables o en acuerdos delegatorios, cuenten con la facultad expresa para requerir la localización geográfica en tiempo real de los equipos de comunicación, así como la entrega de los datos conservados”, y son las únicas que pueden requerir información a las empresas telefónicas, quienes tendrán la obligación legal de proporcionarla.

La Ley Federal de Telecomunicaciones y Radiodifusión mandata, en el artículo 189, que las empresas de telecomunicaciones están obligadas a atender todo

[43] Apartado realizado con base en Congreso de la Unión, *Ley Federal de Telecomunicaciones y Radiodifusión*, México, *Óp. Cit.,* e Instituto Federal de Telecomunicaciones, *Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996*, *Óp. Cit.*

mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezca la normatividad.

De igual forma, tienen la obligación de colaborar con las instancias de seguridad, procuración y administración de justicia en la localización geográfica en tiempo real de equipos de comunicación móvil. Cualquier omisión o desacato será sancionado en los términos de la legislación penal aplicable (Ley Federal de Telecomunicaciones y Radiodifusión, artículo 190, fracción I).

Para cumplir con lo establecido anteriormente, las empresas telefónicas tienen la obligación de conservar los datos de las comunicaciones desde la fecha en que se hayan producido hasta los primeros doce meses para la consulta y entrega de información de manera inmediata. Concluido ese plazo, se deberá conservar por doce meses adicionales en sistemas de almacenamiento electrónico, de suerte que sean entregados a más tardar dentro de las cuarenta y ocho horas siguientes a la petición autorizada (Ley Federal de Telecomunicaciones y Radiodifusión, artículo 190, fracción II).

Queda prohibida la utilización de los datos conservados para fines distintos a los previstos (Ley Federal de Telecomunicaciones y Radiodifusión, artículo 190, fracción III). Asimismo, las empresas deberán contar con un área responsable las veinticuatro horas del día durante los trescientos sesenta y cinco días del año para atender los requerimientos en la materia (Ley Federal de Telecomunicaciones y Radiodifusión, artículo 190, fracción IV).

El área responsable es entonces aquella designada por las empresas para la atención de los requerimientos de las autoridades sobre localización geográfica en tiempo real de los equipos de comunicación móvil, entrega de datos conservados, así como intervención de comunicaciones privadas (Lineamientos, artículo segundo, párrafo I).

Asimismo, las empresas deberán contar con una plataforma electrónica que garantice la seguridad e integridad de la información a efecto de proporcionar los datos solicitados o, en caso de que hayan convenido otros instrumentos o

mecanismos con dichas autoridades, éstos deberán garantizar la seguridad e integridad de ésta (Lineamientos, artículo octavo, fracción I).

A la plataforma podrán tener acceso las autoridades designadas sin tener restricción de ningún tipo, donde estará disponible la información actualizada que sea autorizada por el juez de control (Lineamientos, artículo séptimo, apartado A, fracción II).

Los Lineamientos incluyen al respecto el proceso para atender los requerimientos de las modalidades de datos conservados y localización geográfica en tiempo real, así como lo relativo a la transparencia y protección de datos personales de la información a la que hace referencia.

2.4. Consideraciones finales del capítulo

Como se desprende de lo anterior, en la legislación mexicana se identificaron cuatro definiciones sobre intervención de comunicaciones privadas: 1) Ley Federal Contra la Delincuencia Organizada (1996); 2) Ley de Seguridad Nacional (2005); 3) Código Nacional de Procedimientos Penales (2014); y 4) Código Militar de Procedimientos Penales (2016).

Éstas coinciden en una serie de aspectos fundamentales como son el tipo de dispositivo o tecnología que es susceptible de ser intervenida, sea actual o nueva; el tipo de comunicación que puede ser oral, escrita, etc.; el tipo de acción relativa a los verbos rectores que pueden ser actualizados por la autoridad responsable; y la temporalidad que puede ser en tiempo real o con posterioridad al proceso comunicativo. Aunque no existe una definición única, sí se aportan los elementos torales para su uso por parte de las instituciones.

En cuanto a las modalidades, existen cuatro reconocidas en la ley: 1) los datos conservados que consisten en la información que tiene en resguardo las empresas telefónicas asociadas con líneas fijas, servicios móviles y modalidad de prepago; 2) la localización geográfica en tiempo real que podrá ser entregada de acuerdo con

la frecuencia que requiera la autoridad en términos de horas, minutos, etc.; 3) la extracción de información de dispositivos electrónicos para obtener datos de texto, audio, imagen o video de cualquier dispositivo tecnológico; y 4) las escuchas que consisten en el monitoreo, grabación, registro o conservación de contenido sobre conversaciones. Las modalidades anteriores permiten obtener datos que se desprendan de las comunicaciones para la prevención, investigación y persecución de delitos.

Adicionalmente, deberían incluirse o reconocerse otras modalidades relacionadas con mensajes, llamadas y videollamadas por internet, aplicaciones tecnológicas, buscadores y páginas web. Esto con el fin de regular la operación de empresas extrajeras y actualizar la legislación de acuerdo con la evolución tecnológica y de comunicaciones.

La legislación en la materia también obliga a las empresas telefónicas a cooperar con las instancias de procuración de justicia, seguridad pública y seguridad nacional de acuerdo con lo establecido en el marco legal. De hecho, tendrán una oficina disponible las veinticuatro horas del día durante los trescientos sesenta y cinco días del año, con la finalidad de facilitar la información autorizada por el juez. En caso de que exista la omisión de una obligación o desacato podrán ser sancionados administrativa y/o penalmente.

Una vez revisada le legislación nacional e internacional aplicable a las intervenciones de comunicaciones privadas a lo largo del primer capítulo y establecida la definición y modalidades en el segundo, el siguiente apartado tiene como propósito hacer un reconocimiento y un mapeo de las áreas dentro de las instituciones en materia de procuración de justicia, seguridad pública y seguridad nacional donde se implementan las intervenciones de acuerdo con una revisión legal y de literatura especializada.

Capítulo 3. Análisis legal - institucional de las intervenciones de comunicaciones privadas utilizadas en dependencias de procuración de justicia, seguridad pública y seguridad nacional

El capítulo 3 tiene el objetivo de identificar las instituciones y áreas que realizan las intervenciones de comunicaciones privadas a nivel federal en materia de seguridad pública, seguridad nacional y procuración de justicia. Esto se hace a partir de la revisión de los ordenamientos jurídicos, documentos especializados y fuentes abiertas.

Cabe señalar que la revisión de las instituciones únicamente se plantea a nivel federal, no a nivel de las entidades federativas. En ese sentido, se abordan la FGR, la GN, el CNI, la SEDENA y la SEMAR. Esto con la finalidad de delimitar temáticamente la tesina, pues la revisión de los casos locales en el país implicaría una investigación mucho más extensa.

Sin profundizar, parte de la intención del capítulo es contrastar el ámbito formal-institucional con la implementación de las intervenciones de manera práctica. Hacia el final del apartado se abordan aspectos generales relacionados con un posible mal uso de las tecnologías de intervenciones para obtener información sensible de personas u objetivos relevantes (“espionaje”) en ámbitos políticos, económicos, de medios de comunicación, entre otros, lo cual destaca la necesidad de fortalecer el marco jurídico en la materia.

3.1. Procuración de Justicia

3.1.1. Fiscalía General de la República (FGR)

En la Ley Federal Contra la Delincuencia Organizada, se establece en el artículo 8, que la FGR contará con “una unidad especializada en la investigación y procesamientos de delitos cometidos por personas que formen parte de la

delincuencia organizada, integrada por agentes del Ministerio Público de la Federación, quienes tendrán bajo su mando y conducción a policías y peritos".[44]

Esta unidad contará con un "cuerpo técnico que ejecutará los mandatos de la autoridad judicial que autoricen las intervenciones y verificará la autenticidad de los resultados; establecerá lineamientos sobre las características de los aparatos, equipos y sistemas a autorizar; así como sobre la guardia, conservación, mantenimiento y uso de los mismos".[45]

Actualmente, de acuerdo con la Ley de la Fiscalía General de la República, el Manual de Organización y Procedimientos de la FGR, y el Estatuto Orgánico, son varias las áreas relacionadas con las intervenciones de comunicaciones privadas:

- **Fiscalía Especializada en materia de Delincuencia Organizada (FEMDO)**. Cuenta con la Unidad de Cuerpo Técnico de Control que "gestiona, ejecuta y registra los actos de investigación consistentes en la intervención de comunicaciones privadas en sus diversas modalidades, con autorización judicial, […] coordina la entrega de los registros y control de comunicaciones, y supervisa el uso y conservación de equipos, aparatos y sistemas asignados para el ejercicio de sus facultades".[46]

  En el Estatuto Orgánico de la FGR, en el artículo 90, se señalan las facultades del Cuerpo Técnico de Control, entre las cuales resaltan el realizar las intervenciones; el manejo de aparatos, equipos y sistemas tecnológicos relacionados; la coordinación con las concesionarias de telecomunicaciones; y la transcripción de audios derivados de estos actos de investigación.
- **Agencia de Investigación Criminal (AIC)**. Tiene adscrita la Unidad de Técnicas de Investigación que también "gestiona, ejecuta y registra los actos

[44] Congreso de la Unión, *Ley Federal contra la Delincuencia Organizada*, México, publicada en el Diario Oficial de la Federación el 07 de noviembre de 1996, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFCDO.pdf [consulta: noviembre, 2023].
[45] *Ibidem*.
[46] Fiscalía General de la República. *ACUERDO A/001/2023 por el que se emite el Manual de Organización y Procedimientos de la Fiscalía General de la República*, México, publicado en el Diario Oficial de la Federación el 09 de octubre de 2023, dirección URL: https://sidof.segob.gob.mx/notas/5704316 [consulta: noviembre, 2023].

de investigación consistentes en la intervención de comunicaciones privadas en sus diversas modalidades, que no sean competencia de la Unidad de Cuerpo Técnico de Control; coordina la entrega de los registros y control de comunicaciones; supervisa el uso y conservación de equipos, aparatos y sistemas asignados, y establece directrices sobre sus características" [47].

- **Centro Federal de Inteligencia Criminal (CFIC)**. El Estatuto Orgánico otorga la facultad a la persona titular del Centro Federal de Inteligencia Criminal de supervisar las técnicas y actos de investigación relacionados, y de solicitar los reportes operativos y administrativos necesarios para verificar la autenticidad de los contenidos resultantes de las intervenciones.

De esta forma, serían tres áreas las encargadas formalmente de la realización de las intervenciones de comunicaciones privadas en la FGR: FEMDO, AIC y CFIC. Sin embargo, esto no quita la posibilidad que otras Fiscalías Especializadas o las delegaciones estatales de la dependencia puedan solicitarlas.

En diciembre de 2023, la FGR emitió un acuerdo donde el titular de la institución delega en los agentes del Ministerio Público de la Federación diversas facultades, entre las que se encuentran el:

> *"…Solicitar al órgano jurisdiccional competente, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen la localización geográfica en tiempo real o la entrega de datos conservados, en términos de lo previsto en los artículos 303 del Código Nacional de Procedimientos Penales o 133 Quáter del Código Federal de Procedimientos Penales, según corresponda…".*[48]

Por su parte, la Ley Federal de Transparencia y Acceso a la Información Pública, en el artículo 69, fracción V, inciso a), señala que, en materia de procuración de

---

[47] *Ibidem*.

[48] Fiscalía General de la República, *ACUERDO POR EL QUE SE DELEGAN DIVERSAS FACULTADES EN LAS PERSONAS AGENTES DEL MINISTERIO PÚBLICO DE LA FEDERACIÓN*, México, 06 de diciembre de 2023, dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5710651&fecha=06/12/2023#gsc.tab=0 [consulta: diciembre, 2023].

justicia, la FGR y sus homólogas locales deben de emitir periódicamente la estadística sobre:

> *"…[El] listado de solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de Internet para la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, que contenga exclusivamente el objeto, el alcance temporal y los fundamentos legales del requerimiento, así como, en su caso, la mención de que cuenta con la autorización judicial correspondiente…".*

En ese sentido, en agosto de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) instruyó a la FGR entregar versiones públicas de las solicitudes y requerimientos de intervenciones del 1° de enero de 2018 al 31 de diciembre de 2020, como parte de la vigilancia ciudadana a este tipo de técnicas. Lo anterior debido a que la invasión y el control que se podría tener sobre una persona debe encontrarse apegado al marco legal correspondiente.[49] Actualmente el histórico de la información estadística relacionada con las intervenciones está disponible en la Plataforma Nacional de Transparencia del INAI.[50]

En otro orden de ideas, de la búsqueda de información en medios, se identificó que entre 2019 y 2020, derivado de una revisión de la Auditoría Superior de la Federación (ASF), la FGR habría adquirido a través de empresas intermediarias, diversas tecnologías para la realización de intervenciones. Entre ellas, *Geomatrix* por 2.4 millones de dólares, con lo que se tiene la capacidad de hacer hasta 255 mil búsquedas de geolocalizaciones en tiempo real.[51]

---

[49] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *INAI instruye a FGR informar sobre intervención de comunicaciones privadas, de 2018 a 2020*, México, 08 de agosto de 2021, dirección URL: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-066-21.pdf [consulta: diciembre, 2023].

[50] Plataforma Nacional de Transparencia. *Intervención de comunicaciones privadas*, actualizado a diciembre de 2023, dirección URL: https://consultapublicamx.plataformadetransparencia.org.mx/vut-web/faces/view/consultaPublica.xhtml#tarjetaInformativa [consulta: diciembre, 2023].

[51] Gallegos, Zorayda, "La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles", en *El País*, México, 14 de abril de 2021, dirección URL: https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html [consulta: diciembre, 2023] y Red en

De acuerdo con el diario *El País* también se suscribieron contratos, entre 2019 y 2020, relacionados con la consulta y análisis de datos masivos sobre personas usuarias de internet, sin requerir la colaboración del individuo ni de las plataformas de internet, aplicaciones o contenidos, a través de la plataforma *Echo*. [52]

3.2. Seguridad Pública

3.2.1. Guardia Nacional (GN)

En la Ley de Guardia Nacional, el artículo 100 indica que será el Comandante o titular de la Jefatura de la Coordinación Policial[53] quien podrá solicitar estos actos de investigación ante el órgano judicial.[54] Por su parte, el Reglamento de la Ley de GN establece que será la Dirección General de Inteligencia el área que tiene como atribución el "rendir los informes sobre los resultados de las intervenciones de comunicaciones privadas ante la autoridad judicial" (artículo 33, fracción XXXVII).[55]

En tanto que el Manual de Organización de la GN publicado en septiembre de 2021, señala que la Dirección General de Inteligencia tiene como funciones solicitar la intervención de comunicaciones al Comandante de la GN o a la persona titular de la Jefatura General de Coordinación Policial; rendir los informes sobre los resultados de las intervenciones con la finalidad de hacerlos del conocimiento de los Ministerios Públicos; y proponer al Comandante de la GN las disposiciones sobre el levantamiento de las actas circunstanciadas derivadas de la intervención de

---

Defensa de los Derechos Digitales, "#FISCALÍAESPÍA: LA FGR ADQUIRIÓ EQUIPO CAPAZ DE ESPIAR ILEGALMENTE A TODOS LOS USUARIOS DE INTERNET EN MÉXICO", México, 14 de abril de 2021, dirección URL: https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/ [consulta: diciembre, 2023].

[52] *Ibidem*.

[53] De acuerdo con el Reglamento de la Ley de GN, artículo 20, la Jefatura de la Coordinación Policial es el órgano técnico operativo, colaborador inmediato del Comandante, a quien auxilia en la concepción, planeación y conducción de las atribuciones policiales, para transformar sus decisiones en órdenes, e instrucciones y verificar su cumplimiento. *Vid*. Congreso de la Unión, *Ley de la Guardia Nacional*, México, publicada en el Diario Oficial de la Federación el 27 de mayo de 2019, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf [consulta: noviembre, 2023].

[54] *Ibidem*.

[55] Congreso de la Unión, *Reglamento de la Ley de la Guardia Nacional*, México, publicada en el Diario Oficial de la Federación el 29 de junio de 2019, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGN_111220.pdf [consulta: noviembre, 2023].

comunicaciones con fecha de inicio y término, un inventario de documentos y cintas de audio o video con sonidos o imágenes captadas durante las mismas.

Por su parte, la Dirección General de Vigilancia y Supervisión Interna tiene, entre sus atribuciones, el supervisar que el desempeño de los integrantes en las intervenciones se haya ajustado a las disposiciones jurídicas aplicables una vez concluida la técnica.[56]

Recientemente, en el *Acuerdo por el que se crea la Subjefatura de Investigación e Inteligencia de la Guardia Nacional*, publicado en el DOF el 28 de septiembre de 2023, se indica que esta área tiene entre sus funciones el proponer al titular de la Jefatura General de Coordinación Policial la intervención de comunicaciones privadas.[57]

De esta forma, serían diversas las áreas involucradas en las intervenciones por parte de GN:

- Comandante General
- Jefatura General de Coordinación Policial
- Subjefatura de Investigación e Inteligencia
- Dirección General de Inteligencia
- Dirección General de Vigilancia y Supervisión Interna

Cabe destacar que, en junio de 2019, la Comisión Nacional de Derechos Humanos (CNDH) promovió una acción de inconstitucionalidad 62/2019 contra varios artículos de la Ley de Guardia Nacional, que reconocían la posibilidad de realizar tareas de investigación, solicitudes de información de datos conservados, geolocalizaciones de teléfonos celulares, acciones de vigilancia, monitoreo, rastreo e intervención de

[56] *Ibidem*.
[57] Secretaría de Seguridad y Protección Ciudadana, *ACUERDO por el que se crea la Subjefatura de Investigación e Inteligencia de la Guardia Nacional*, México, 28 de septiembre de 2023, dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5703227&fecha=28/09/2023#gsc.tab=0 [consulta: noviembre, 2023].

comunicaciones "*so pretexto* de prevenir conductas delictivas e infracciones administrativas".[58] La CNDH refirió que:

> *"…las disposiciones referidas, resultan lesivas de los derechos fundamentales reconocidos por el Estado mexicano, como a la intimidad, privacidad y prohibición de injerencias arbitrarias, ya que los elementos de la Guardia Nacional realicen actos de investigación, verificación, georreferenciación, intervención de comunicaciones en materia de prevención de los delitos e infracciones administrativas. Dada la amplitud e indeterminación de dichas facultades, se da pauta a la arbitrariedad y discrecionalidad por parte dichas autoridades, por lo que resultan contrarias al derecho de seguridad jurídica y del principio de legalidad…".*

Como resultado del análisis, en abril de 2023, el pleno de la SCJN invalidó el artículo 9, fracción VI, donde se permitía a la institución realizar operaciones encubiertas y usuarios simulados.[59]

No obstante, validó diversos preceptos de la ley, entre ellos los relativos a actividades como "…b) recabar información en lugares públicos; obtener, analizar y procesar información; así como realizar acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de internet, en los tres casos, con el fin de prevenir conductas delictivas […] c) solicitar a la autoridad judicial la intervención de comunicaciones para la prevención del delito…".[60]

Con ello, como resultado de la acción de inconstitucionalidad 62/2019 promovida por la CNDH, se dieron por válidas facultades de la institución relacionadas con la intervención de comunicaciones privadas con la finalidad de prevenir delitos por parte de GN.[61]

---

[58] Comisión Nacional de los Derechos Humanos, *Demanda de acción de inconstitucionalidad, promovida por la CNDH*, México, 26 de junio de 2019, dirección URL: https://www.cndh.org.mx/sites/default/files/documentos/2019-07/Acc_Inc_2019_62.pdf [consulta: diciembre, 2023].
[59] Suprema Corte de Justicia de la Nación, SCJN ANALIZA DIVERSAS DISPOSICIONES DE LA LEY DE LA GUARDIA NACIONAL, México, 24 de abril de 2023, dirección URL: https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=7333 [consulta: diciembre, 2023].
[60] *Ibidem*.
[61] *Ibidem*.

De acuerdo con fuentes periodísticas, entre 2020 y 2021, la GN intervino 685 veces comunicaciones privadas a partir de información brindada por empresas como AT&T, Movistar, Telcel y Telmex. De éstas, 249 se realizaron en 2021 y 436 en 2020.[62]

En 2022, la dependencia habría solicitado a la Secretaría de Hacienda y Crédito Público, a través de diferentes proyectos, la adquisición de una plataforma para la intervención de comunicaciones privadas y para equipos de localización de celulares para el combate a la delincuencia organizada, con un costo de 846 millones de pesos. Concretamente se trata de una petición de la Dirección General de Inteligencia que impulsó un proyecto denominado "Adquisición de herramientas tecnológicas para la obtención de información".[63]

En 2023, también la Dirección General de Inteligencia habría solicitado 67 millones de pesos para interceptar y grabar, como mínimo, 50 líneas telefónicas simultáneas y 500 objetivos. Actualmente esta área contaría, de acuerdo con información periodística, con 288 líneas analógicas activadas para grabar 50 líneas en vivo con una capacidad de almacenamiento de grabación de 180 días.[64]

3.3. Seguridad Nacional

En materia de seguridad nacional el CNI, la SEDENA y la SEMAR coinciden en un aspecto fundamental: existe poca información pública sobre el funcionamiento de estas dependencias en materia de intervención de comunicaciones privadas. No obstante, se hizo un esfuerzo por indagar a partir de los documentos oficiales

[62] Cabrera, David, "GN solicitó 67 mdp para intervenir comunicaciones de 500 objetivos", en *La Otra Opinión, México – Ricardo Alemán*, 08 de septiembre de 2022, dirección URL: https://laotraopinion.com.mx/gn-solicito-67-mdp-para-intervenir-comunicaciones-de-500-objetivos/ [consulta: diciembre, 2023].
[63] Vega, Carlos, "Guardia Nacional gestiona 846 mdp para inteligencia anticrimen", en *Milenio*, México, 28 de octubre de 2022, dirección URL: https://www.milenio.com/policia/guardia-nacional-gestiona-846-mdp-inteligencia-anticrimen [consulta: diciembre, 2023].
[64] Redacción, "Guardia Nacional pidió 67.1 mdp para equipo de intervención de comunicaciones", en *Aristegui Noticias*, México, 07 de septiembre de 2022, dirección URL: https://aristeguinoticias.com/0709/mexico/guardia-nacional-pide-dinero-para-intervenir-comunicaciones-de-500-objetivos/ [consulta: diciembre, 2023].

disponibles, de investigaciones periodísticas y de documentos especializados, el funcionamiento de las intervenciones dentro de las dependencias señaladas.

3.3.1. Centro Nacional de Inteligencia (CNI)

En la Ley de Seguridad Nacional que regula el funcionamiento del CNI, no se abordan las áreas particulares encargadas de realizar las intervenciones. Dada la naturaleza de secrecía en el funcionamiento de la institución y en el manejo de la información, es difícil identificar las secciones específicas en las que se realizan las intervenciones.

No obstante, existen algunas publicaciones en fuentes abiertas que dan una idea general sobre dónde y cómo se podrían implementar. El CNI se organiza para su operación en siete áreas sustantivas:[65]

- Coordinación General de Contrainteligencia
- Coordinación General de Análisis
- Coordinación General de Operaciones
- Coordinación General Jurídica
- Coordinación General de Investigación
- Coordinación General Administrativa
- Coordinación General de Servicios Técnicos

Específicamente la Coordinación de Servicios Técnicos tiene adscritas dos áreas posiblemente relacionadas con las intervenciones de comunicaciones privadas: 1) la Dirección de Intervenciones y 2) la Dirección de Desarrollo Tecnológico. Sin embargo, no se identificó información pública sobre la operación de la Dirección de Intervenciones para profundizar sobre la estructura, funcionamiento o actividades.

[65] Badillo, Miguel, “La nueva estructura y los salarios del Centro Nacional de Inteligencia”, en *Contralínea*, México, 06 de mayo de 2023, dirección URL: https://contralinea.com.mx/interno/semana/la-nueva-estructura-y-los-salarios-del-centro-nacional-de-inteligencia/ [consulta: diciembre, 2023].

Sobre el particular, diversos medios de comunicación han hecho un seguimiento sobre las actividades del CNI relacionados con las intervenciones. El entonces Centro de Investigación y Seguridad Nacional (CISEN), antecedente directo del CNI, solicitó ante el órgano judicial, entre diciembre de 2006 y 2017, 3 mil 813 autorizaciones para intervenir comunicaciones privadas, de las cuales los jueces autorizaron 3 mil 813 y rechazaron 83.[66]

En contraste, de acuerdo con la Plataforma Nacional de Transparencia, desde el cambio de gobierno en diciembre de 2018 y al menos hasta 2021, no se encontró "un solo registro de solicitud de intervención telefónica ni petición para extraer datos de aparatos telefónicos de ciudadanos".[67]

Esto parece ser poco verosímil, en el sentido que es complicado que el órgano de inteligencia civil del Estado mexicano no realice intervención de comunicaciones en alguna de sus modalidades. Como hipótesis, existe la posibilidad que éstas se realicen sin control judicial y que por ello no quede registro en la Plataforma Nacional de Transparencia.

3.3.2. Fuerzas Armadas

Se realizó una búsqueda de la normatividad de las Fuerzas Armadas, incluyendo la SEDENA y la SEMAR, y únicamente dos ordenamientos regulan esta situación.

Por un lado, como se estableció en el capítulo 1, las intervenciones que reconoce el Código Militar de Procedimientos Penales (CMPP) son únicamente respecto de hechos que se investigan probablemente cometidos por personal militar, en el ámbito de competencia castrense. Es decir, el ordenamiento no regula el uso de intervenciones para la investigación de delitos del fuero civil desde el ámbito militar.

---

[66] Camacho, Zózimo, "Cisen: 11 años de comunicaciones intervenidas", en *Contralínea*, México, 11 de octubre de 2017, dirección URL: https://contralinea.com.mx/noticias/cisen-11-anos-comunicaciones-intervenidas/ [consulta: diciembre, 2023].

[67] Castillo, Gustavo y Murillo, Eduardo, "Al llegar AMLO cesaron peticiones de intervención telefónica", en *La Jornada*, México, 22 de julio de 2021, dirección URL: https://www.jornada.com.mx/notas/2021/07/22/politica/al-llegar-amlo-cesaron-peticiones-de-intervencion-telefonica/ [consulta: diciembre, 2023].

Por su parte, en el Código de Justicia Militar (CJM), en el artículo 49 Bis, fracción XIII, señala que la Policía Ministerial Militar actuará bajo la conducción y el mando del Ministerio Público, y podrá solicitar las intervenciones "exclusivamente respecto del personal militar", previa autorización de la autoridad judicial federal.

Sobre estos ordenamientos, en abril de 2023, la Suprema Corte de Justicia invalidó varios artículos del CMPP y del CJM que permitían a las autoridades militares llevar a cabo intervenciones sin autorización de un juez civil. Esto fue resultado de la acción de institucionalidad 46/2016 que presentó la CNDH, con lo cual se invalidaron diversos artículos, siendo los principales el 299 del CMPP y 81 bis, fracción VII, y el 83 fracción XIII del CJM. Lo anterior con la intención que, bajo cualquier supuesto, las intervenciones solicitadas por las Fuerzas Armadas tengan que pasar por un control constitucional en el fuero civil, es decir, del Centro Nacional.[68]

El artículo 299 del CMPP, invalidado por la SCJN, regulaba la localización geográfica en tiempo real, respecto de hechos que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia de la justicia castrense.

En tanto, el artículo 81 bis, fracción VII, mencionaba que el Fiscal General durante su ausencia podía delegar al Fiscal General Adjunto, al Fiscal Militar Auxiliar y al Fiscal Militar de Investigación del Delito y Control de Procesos:

> *"…[El] solicitar previa autorización judicial a los concesionarios o permisionarios o comercializadoras del servicio de telecomunicaciones o comunicación vía satélite, la localización geográfica en tiempo real de los equipos de comunicación móvil asociados a una línea que se encuentren relacionados exclusivamente con los hechos que se investigan a personal militar en el ámbito de su competencia y en términos del Código Militar de Procedimientos Penales…".*

[68] Red en Defensa de los Derechos Digitales, *CORTE INVALIDA INTERVENCIÓN DE COMUNICACIONES PRIVADAS POR MILITARES SIN AUTORIZACIÓN DE UN JUEZ CIVIL*, México, 17 de abril de 2023, dirección IRL: https://r3d.mx/2023/04/17/corte-invalida-intervencion-de-comunicaciones-privadas-por-militares-sin-autorizacion-de-un-juez-civil/ [consulta: diciembre, 2023] y Suprema Corte de Justicia de la Nación, *Síntesis informativa*, México, 18 de abril de 2023, dirección URL: https://www.scjn.gob.mx/sites/default/files/sintesis-informativa/2023-04/S%C3%ADntesisPDF-18abril2023.pdf [consulta: diciembre, 2023].

Sin embargo, como se mencionó, en ambos casos, los artículos y fracciones señaladas fueron declaradas inválidas por sentencia de la SCJN ante la acción de inconstitucionalidad notificada para efectos legales el 19 de julio de 2023 y publicada en el DOF el 05 de septiembre de 2023.

Otro de los aspectos que resulta fundamental establecer es que la normatividad de las Fuerzas Armadas no identifica, ni siquiera de manera general, qué área de la institución realizará las actividades de intervenciones de comunicaciones privadas. Se revisaron, entre otros, los siguientes ordenamientos sin encontrar referencias al tema en comento:

- Ley Orgánica del Ejército y Fuerza Área Mexicanos
- Reglamento Interior de la SEDENA
- Manual de Organización de la SEDENA
- Ley Orgánica de la Armada de México
- Reglamento Interior de la SEMAR
- Manual General de Organización de la SEMAR

Se podría interpretar que dentro de SEDENA, como parte de las actividades de inteligencia, dentro del Estado Mayor, la Sección Segunda encargada de la Jefatura de Inteligencia, sería la responsable en la implementación de las intervenciones. Esta área se integraría por: Subsección de Información, Subsección de Inteligencia, Subsección de Contrainteligencia, y Subsección de Protocolo y Enlace con el Extranjero.[69] Igualmente realizaría estas operaciones el Centro de Inteligencia Militar (CIM), también dependiente del Estado Mayor.[70]

De hecho, ante peticiones de información pública sobre las solicitudes realizadas por SEDENA ante el Poder Judicial de la Federación para la realización de

[69] Mendoza Cortés, Paloma, “Inteligencia y contrainteligencia militar frente a fallos y desafíos. El caso de Culiacán, México (2019)”, en *Revista Latinoamericana de Estudios de Seguridad*, N° 26, FLACSO Ecuador, enero de 2020.
[70] Tourliere, Mathieu, “Centro Militar de Inteligencia, el búnker de la 4T para espiar”, en *Revista Proceso*, México, 11 de marzo de 2023, dirección URL: https://www.proceso.com.mx/reportajes/2023/3/11/centro-militar-de-inteligencia-el-bunker-de-la-4t-para-espiar-303474.html [consulta: diciembre, 2023].

intervención de comunicaciones, la institución señaló que “no se localizó expresión documental que atienda la solicitud” para el periodo del 1 de enero de 2018 al 31 de mayo de 2022. En palabras simples, en el periodo referido, la institución no ha hecho intervenciones de comunicaciones legales.[71]

Por su parte, en la SEMAR, la Unidad de Inteligencia Naval (UIN) sería la encargada de realizar estas actividades, dado que tiene entre sus funciones operar un sistema de inteligencia que apoye al titular en la toma de decisiones; identificar amenazas a la seguridad nacional; incorporar nuevas tecnologías que optimicen las actividades de inteligencia; y establecer estrategias de contrainteligencia, entre otras.[72] Sin embargo, no se tiene certeza que sea de esta forma.

Una de las conclusiones preliminares en el ámbito de la seguridad nacional, por lo que respecta al CNI, SEDENA y SEMAR, es que carecen de un marco legal que dé certeza jurídica a los ciudadanos del tipo de actividades, áreas específicas, responsables, procedimientos y, en general, de las facultades con las que cuenta las dependencias en términos de las intervenciones de comunicaciones privadas que se podrían realizar a civiles.

En ese mismo sentido, las actividades de intervenciones que realicen las Fuerzas Armadas no podrían ser tomadas como elementos probatorios para juicios de naturaleza penal. Al carecer de un marco legal, su obtención y presentación ante el órgano judicial sería prueba ilícita y carecería de todo valor.

Por tanto, es necesario que el legislador colme este vacío jurídico que es un riesgo para la realización de actividades que pueden considerarse como “espionaje” por parte de estas dependencias y que, en algún punto, podrían configurar un delito realizado por personal castrense. Lo anterior con la intención de dar certeza jurídica a las Fuerzas Armadas en su actuación y a los ciudadanos.

---

[71] Tourliere, Mathieu, “Centro Militar de Inteligencia, el búnker de la 4T para espiar”, *Óp. Cit.*

[72] Secretaría de Marina, *ACUERDO Secretarial número 172, por el que se expide el Manual de Organización General de la Secretaría de Marina*, México, publicado en el Diario Oficial de la Federación el 29 de julio de 2016, dirección URL: https://dof.gob.mx/nota_detalle.php?codigo=5446206&fecha=29/07/2016#gsc.tab=0 [consulta: diciembre, 2023].

Para complementar este apartado relativo a seguridad nacional, es necesario decir que la Ley Federal de Telecomunicaciones y Radiodifusión, en el artículo 190, fracción XII, señala que el IFETEL realizará:

> *"…Los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Los concesionarios que operen redes públicas de telecomunicaciones podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones. Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Instituto, al Congreso de la Unión y al Ejecutivo Federal".*

En el mismo sentido, los Lineamientos de Colaboración en Materia de Seguridad y Justicia, en el Capítulo X "De los Estudios de Investigaciones que Permitan Inhibir y Combatir la Utilización de Equipos Tecnológicos para la Comisión de Delitos o Actualización de Riesgos o Amenazas a la Seguridad Nacional", establecen que las empresas involucradas en coordinación con el IFETEL realizarán estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional.

3.4. ¿Espionaje y violación a los derechos humanos?

En el contexto explicado anteriormente, es ineludible abordar, aunque sea brevemente, una temática que se presenta de manera consistente en los últimos años en México: el espionaje. De acuerdo con la definición de la Real Academia de la Lengua Española es la "actividad secreta encaminada a obtener información sobre un país, especialmente en lo referente a su capacidad defensiva y ofensiva" o la "actividad dedicada a obtener información fraudulenta en diversos campos".[73]

[73] Real Academia de la Lengua Española*, Definición: espionaje*, España, dirección URL: https://dle.rae.es/espionaje [consulta: diciembre, 2023].

En términos de esta tesis, el espionaje puede ser definido como la actividad sistemática realizada por individuos, dependencias públicas o privadas, tendiente a obtener datos o información relevante de manera ilegal (es decir, sin autorización previa de la persona y/o sin orden judicial), sobre las actividades realizadas por un individuo, colectividades, corporaciones públicas o privadas, dependencias gubernamentales, así como por otras entidades objeto de interés (como pudiera ser el ámbito industrial, empresarial o científico).

Diversos medios de comunicación han documentado actividades sobre el presunto espionaje en México, tanto desde el ámbito civil como del militar. De acuerdo con el diario británico *The Guardian* aproximadamente 15 mil líneas telefónicas fueron intervenidas ilegalmente desde 2016 hasta 2021, pertenecientes a activistas de derechos humanos, periodistas, políticos, empresarios y abogados.[74]

Para realizar esta actividad la firma israelí *NSO Group* comercializó al gobierno mexicano el *malware*[75] Pegasus. Éste es un programa computacional que al ser instalado en un teléfono (sin importar si es iOS o Android), permite que el dispositivo se convierta en una herramienta de espionaje a control remoto. Es posible leer mensajes de texto, revisar fotos o conocer la ubicación en tiempo real, incluso se pueden activar las cámaras o los micrófonos sin que los usuarios lo detecten.[76]

Este sistema a nivel internacional se habría implementado cuando menos en 50 países teniendo como objetivos a más de 500 diplomáticos, más de mil 200

---

[74] Monroy, Jorge, "15,000 números telefónicos de México fueron detectados en lista de malware de espionaje Pegasus: The Guardian", en *El Economista*, México, 18 de julio de 2021, dirección URL: https://www.eleconomista.com.mx/politica/15000-numeros-telefonicos-de-Mexico-fueron-detectados-en-lista-de-malware-de-espionaje-Pegasus-The-Guardian-20210718-0025.html [consulta: diciembre, 2023] y Garduño, Mónica, "Así logró el software Pegasus espiar a 25 periodistas mexicanos", en *Forbes*, México, 21 de julio de 2021, dirección URL: https://www.forbes.com.mx/tecnologia-asi-software-pegasus-espiar-25-periodistas-mexicanos/ [consulta: diciembre, 2023].

[75] De acuerdo con Microsoft, un *malware* "hace referencia a aplicaciones o código malintencionados que dañan o alteran el uso habitual de los dispositivos de punto de conexión. Cuando un dispositivo se infecta con *malware*, puede que se tenga acceso a él sin autorización, que los datos se pongan en peligro o que se te impida el acceso al dispositivo salvo que pagues un rescate". *Ver*. Microsoft, ¿Qué es el *malware*?, dirección URL: https://www.microsoft.com/es-mx/security/business/security-101/what-is-malware [consulta: diciembre, 2023].

[76] Monroy, Jorge, "15,000 números telefónicos de México fueron detectados en lista de *malware* de espionaje Pegasus: The Guardian", *Óp. Cit.*

funcionarios, alrededor de 250 defensores de derechos humanos y por lo menos 180 periodistas.[77]

La Secretaría de Seguridad y Protección Ciudadana indicó que en México el programa se adquirió en 2014 y su licencia habría vencido en 2017, así como que ésta no fue renovada por el gobierno federal.[78] En 2021, la dependencia aclaró que ni la GN ni el CNI contaban con una licencia vigente. Empero, la evidencia disponible públicamente contravino esta afirmación.

En 2023, según diario *The New York Times*, la SEDENA era la única institución que operaba Pegasus. El primer contrato celebrado por la dependencia con *NSO Group* fue firmado en 2011 y la institución reconoció haberlo utilizado entre ese año y 2013. Posteriormente, se identificaron contratos entre 2015 y 2018.[79]

De acuerdo con la Red en Defensa de los Derechos Digitales (R3D), organización civil dedicada, como su nombre lo indica, a la defensa de los derechos humanos en el entorno digital, sostiene que "…la SEDENA no cuenta con atribuciones legales para realizar intervenciones de comunicaciones privadas; incluso, en la legislación mexicana se contempla que para llevar a cabo estas actividades, las autoridades requieren una autorización judicial, de las que no hay evidencia de que existan…"[80].

---

[77] Senado de la República, *PROPOSICIÓN CON PUNTO DE ACUERDO DE URGENTE Y OBVIA RESOLUCIÓN, POR EL QUE SE SOLICITA AL EJECUTIVO FEDERAL REMITA A ESTA SOBERANIA Y SE HAGA PÚBLICA LA INFORMACIÓN RELATIVA AL ESPIONAJE E INTERVENCION DE COMUNICACIONES PRIVADAS A TRAVÉS DE LA APLICACIÓN PEGASUS DE LA FIRMA TECNOLÓGICA ISRAELI NSO GROUP CONTRATADA POR EL GOBIERNO FEDERAL Y DE OTROS MECANISMOS DE INTERVENCIÓN ILEGAL DE COMUNICACIONES PRIVADAS, Y A LA FISCALIA GENERAL DE LA REPÚBLICA PARA QUE INICIE UNA INVESTIGACIÓN, SE FINQUEN RESPONSABILIDADES Y SE INICIEN LOS PROCESOS JUDICIALES CORRESPONDIENTES*, México, 21 de julio de 2021, dirección URL: https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-07-29-1/assets/documentos/123-PA_Aplicacion-PEGASUS.pdf [consulta: diciembre, 2023].

[78] Monroy, Jorge, "15,000 números telefónicos de México fueron detectados en lista de *malware* de espionaje Pegasus: The Guardian", *Óp. Cit.*

[79] Red en Defensa de los Derechos Digitales, *LO QUE SABEMOS DE LAS AUTORIDADES QUE ADQUIRIERON PEGASUS EN MÉXICO*, México, 23 de julio de 2021, dirección URL: https://r3d.mx/2021/07/23/autoridades-pegasus-mexico/ [consulta: diciembre, 2023].

[80] Red en Defensa de los Derechos Digitales, *LA SEDENA ES ACTUALMENTE EL ÚNICO OPERADOR DE PEGASUS EN MÉXICO, REVELA NYT*, México, 19 de abril de 2023, dirección URL: https://r3d.mx/2023/04/19/la-sedena-es-actualmente-el-unico-operador-de-pegasus-en-mexico-revela-nyt/ [consulta: diciembre, 2023].

El semanario Proceso realizó una investigación en la que indicó que, en SEDENA, el Centro Militar de Inteligencia (CMI) sería el encargado de operar Pegasus. Este centro en 2018 operaba con una plantilla de 293 militares, para 2021 habría pasado a 619. Es decir, durante la actual administración registró un aumento en su personal y operación, sin embargo, esto contrasta con la ausencia de solicitudes de intervenciones por parte de SEDENA ante el Poder Judicial de la Federación.[81]

Además de SEDENA, Pegasus lo habrían adquirido la entonces Procuraduría General de la República (PGR) y el Centro de Inteligencia y Seguridad Nacional (CISEN). El CISEN habría celebrado un contrato en mayo de 2016, mientras que la PGR lo habría adquirido en 2014, con renovación de la licencia en 2016 y 2017.[82]

Diversas organizaciones sociales y periodistas, con el apoyo de *Citizen Lab* de la Universidad de Toronto, documentaron la infección de dispositivos pertenecientes a personas dedicadas a la defensa de los derechos humanos, periodistas, escritores y miembros de la sociedad civil.[83]

A partir de 2021, *NSO Group* habría reducido el número de países a los que puede vender tecnologías de vigilancia de 102 a 32, al no poder comercializar sus productos en países con un "pobre historial de derechos humanos", lo cual cerró la puerta para su adquisición a países como México, Arabia Saudita, Marruecos o Emiratos Árabes.[84]

Si bien Pegasus es el *malware* más conocido y mediático, es necesario mencionar que pudieran existir otros programas de características similares que no han sido suficientemente abordados. Por ejemplo, la empresa de vigilancia *Circles* señaló

---

[81] Tourliere, Mathieu, "Centro Militar de Inteligencia, el búnker de la 4T para espiar", *Óp. Cit.*
[82] Red en Defensa de los Derechos Digitales, *LO QUE SABEMOS DE LAS AUTORIDADES QUE ADQUIRIERON PEGASUS EN MÉXICO*, *Óp. Cit.*
[83] Red en Defensa de los Derechos Digitales, #EJÉRCITOESPÍA: NUEVOS CASOS DE ESPIONAJE CON PEGASUS EN MÉXICO NO DEBEN QUEDAR EN LA IMPUNIDAD, México, 03 de octubre de 2022, dirección URL: https://r3d.mx/2022/10/03/nuevos-casos-de-espionaje-con-pegasus-en-mexico-no-deben-quedar-en-la-impunidad/ [consulta: diciembre, 2023].
[84] Red en Defensa de los Derechos Digitales, *MÉXICO YA NO PODRÍA IMPORTAR TECNOLOGÍAS DE VIGILANCIA DE EMPRESAS ISRAELÍES*, México, 25 de noviembre de 2025, dirección URL: https://r3d.mx/2021/11/25/mexico-ya-no-podria-importar-tecnologias-de-vigilancia-de-empresas-de-israel/ [consulta: diciembre, 2023].

que, entre 2015 y 2020, al menos 10 clientes habrían utilizado su sistema SS7 en México, entre ellos SEMAR. Este sistema es capaz de monitorear redes telefónicas 2G, 3G y 4G, interceptar llamadas, mensajes de texto e identificar la ubicación de dispositivos móviles.[85]

Además está la firma italiana *Hacking Team* que habría comercializado sus servicios a los gobiernos de Baja California y Durango entre 2014 y 2015, así como el sistema *Remote Control* en los estados de Chihuahua, Morelos, Tabasco, Sonora y Yucatán.[86]

Asimismo, se tendría identificada la operación irregular de antenas de telefonía celular con la capacidad de intervenir comunicaciones en diferentes partes del país, operadas por empresas como *L3Harris Technologies* y *South Ligthouse*. Las antenas con más tráfico de comunicaciones estarían ubicadas, primero, en la carretera 115-D que comunica la Ciudad de México con Puebla y Morelos; la segunda, en la autopista México – Marquesa, entre la Ciudad de México y el Estado de México; y, la tercera, en la Plaza de la Constitución, en el primer cuadro de la Ciudad de México.[87]

Lo planteado anteriormente supondría una flagrante violación al artículo 16 constitucional, una constante transgresión a los derechos humanos de las personas y los actos de espionaje que efectivamente se realizan podrían configurar diversas conductas delictivas. No está de más mencionar que existen casos donde

[85] Red en Defensa de los Derechos Digitales, *CITIZEN LAB REVELA USO DE SOFTWARE ESPÍA DE CIRCLES, EMPRESA VINCULADA CON NSO GROUP, EN MÉXICO*, México, 01 de diciembre de 2020, dirección URL: https://r3d.mx/2020/12/01/citizen-lab-revela-uso-de-software-espia-de-circles-empresa-vinculada-con-nso-group-en-mexico/ [consulta: diciembre, 2023].
[86] Red en Defensa de los Derechos Digitales, *EMPRESARIO SE DECLARA CULPABLE DE VENDER EQUIPO DE ESPIONAJE EN MÉXICO A SABIENDAS DE SU USO ILEGAL*, México, 17 de febrero de 2022, dirección URL: https://r3d.mx/2022/02/17/empresario-se-declara-culpable-de-vender-equipo-de-espionaje-en-mexico-a-sabiendas-de-su-uso-ilegal/ [consulta: diciembre, 2023].
[87] Senado de la República, *PROPOSICIÓN CON PUNTO DE ACUERDO DE URGENTE Y OBVIA RESOLUCIÓN, POR EL QUE SE SOLICITA AL EJECUTIVO FEDERAL REMITA A ESTA SOBERANIA Y SE HAGA PÚBLICA LA INFORMACIÓN RELATIVA AL ESPIONAJE…Óp. Cit.*

secretarías y fiscalías locales utilizarían estas técnicas también para la vigilancia de figuras y oponentes políticos.[88]

En ese sentido, la Comisión Interamericana de Derechos Humanos (CIDH), en su *Relatoría Especial para la Libertad de Expresión*, ha hecho un llamado al Estado mexicano para intensificar, de manera urgente, sus esfuerzos en las investigaciones por el uso de Pegasus en contra de periodistas y personas defensoras de los derechos humanos.[89]

Asimismo, a nivel nacional, la CNDH ha alertado sobre un riesgo grave por:

> *"…El ejercicio abusivo de las facultades previstas en la Ley de Seguridad Nacional, el Código Nacional de Procedimientos Penales y el Código Militar de Procedimientos Penales, ya que la redacción actual de estas normas facilita a las autoridades el uso de tecnologías de espionaje tan avanzadas como Pegasus, al ser susceptible de una interpretación subjetiva para justificar, con el discurso de seguridad nacional o investigación de delitos graves, el uso irrestricto de este tipo de tecnología…".*[90]

El tema del espionaje es un tópico ineludible al abordar el tema de las intervenciones de comunicaciones privadas, dado que es fundamental para el desarrollo de un estado de derecho. Si bien podría ser susceptible de una investigación en sí misma, al no ser éste el propósito de la investigación, el espionaje se aborda únicamente de manera general. La intención es resaltar la necesidad de fortalecer el marco jurídico en la materia que tiene claramente áreas susceptibles de mejora.

---

[88] Red en Defensa de los Derechos Digitales, *FISCALÍA DE CDMX ACCEDIÓ A REGISTROS TELEFÓNICOS PARA ESPIAR A FIGURAS POLÍTICAS*, México, 09 de noviembre de 2023, dirección URL: https://r3d.mx/2023/11/09/fiscalia-de-cdmx-accedio-a-registros-telefonicos-para-espiar-a-figuras-politicas/ [consulta: diciembre, 2023].

[89] Red en Defensa de los Derechos Digitales, *LA CIDH MUESTRA PREOCUPACIÓN POR EL ESPIONAJE CON PEGASUS EN MÉXICO*, México, 02 de junio de 2023, dirección URL: https://r3d.mx/2023/06/02/la-cidh-muestra-preocupacion-por-el-espionaje-con-pegasus-en-mexico/ [consulta: diciembre, 2023].

[90] Comisión Nacional de Derechos Humanos, "CNDH emite Recomendación General a autoridades del Estado mexicano por el caso de espionaje y su impacto en la libertad de expresión relacionado con el software Pegasus", México, 26 de mayo de 2022, dirección URL: https://www.cndh.org.mx/sites/default/files/documentos/2022-05/COM_2022_154.pdf [consulta: diciembre, 2023].

Reflexiones finales y recomendaciones sobre las intervenciones de comunicaciones privadas en México

Este apartado tiene como finalidad presentar de manera puntual los principales hallazgos de la tesina de los diferentes capítulos, así como las 11 recomendaciones puntuales derivadas de la investigación.

Capítulo 1.

- La CPEUM reconoce en su artículo 16 la inviolabilidad de las comunicaciones privadas. Únicamente la autoridad judicial federal, a petición del Ministerio Público federal o del titular del Ministerio Público local, podrá autorizar la intervención de cualquier comunicación privada.
- El CNPP establece los procedimientos específicos para la investigación y persecución del delito utilizando las intervenciones de comunicaciones privadas para la FGR y las fiscalías locales.
- La Ley Federal Contra la Delincuencia Organizada indica que la FGR contará con una unidad especializada que ejecutará los mandatos de la autoridad judicial para las intervenciones y verificará su autenticidad. Igualmente, establecerá las características de los aparatos, equipos y sistemas a autorizar, así como la guarda, conservación, mantenimiento y uso de éstos.
- La Ley de Guardia Nacional faculta a la dependencia para realizar las intervenciones con fines de prevención de delitos federales en ilícitos como armas, contra la salud, migración, secuestro, desaparición de personas, trata de personas y otros reconocidos en el Código Penal Federal y otras leyes federales y generales.
- La Ley de Seguridad Nacional regula las facultades del CNI para realizar intervenciones en inteligencia con la intención de prevenir o proteger al Estado Mexicano frente a los riesgos o amenazas a la seguridad nacional.
- En el Código Militar de Procedimientos Penales se regula la actuación de las Fuerzas Armadas respecto de delitos probablemente cometidos por personal militar, exclusivamente en el ámbito de competencia castrense.

- La tesis P. XXXI/2008 emitida por la SCJN señala que existe una imposibilidad constitucional para otorgar valor probatorio a las grabaciones derivadas de las intervenciones de comunicaciones privadas obtenidas sin autorización judicial.
- Por su parte, los instrumentos jurídicos internacionales analizados hacen referencia únicamente al derecho a la privacidad o la prohibición de la interferencia arbitraria de la vida privada, no así propiamente a las intervenciones. Entre otros se encuentran la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, y la Convención Americana sobre los Derechos Humanos.
- No existen actualmente acuerdos bilaterales ni multilaterales en la materia, excepto un tratado con los Estados Unidos que data del año 1987 para la asistencia jurídica mutua en materia penal.

Capítulo 2.

- Se identificaron cuatro definiciones sobre intervenciones de comunicaciones privadas: 1) Ley Federal Contra la Delincuencia Organizada; 2) Ley de Seguridad Nacional; 3) Código Nacional de Procedimientos Penales; y 4) Código Militar de Procedimientos Penales.
- Coinciden en aspectos fundamentales como: aparato o tecnología que es susceptible de ser intervenida incluyendo el avance tecnológico y dispositivos que podrían surgir; tipo de comunicación que puede ser oral, escrita, por señales, etc.; tipo de acción relativa a los verbos rectores que pueden ser actualizados por la autoridad responsable; y la temporalidad en que se pueden aplicar la intervención, sea en tiempo real o con posterioridad al proceso comunicativo.
- Existen cuatro modalidades reconocidas en la ley: 1) datos conservados, 2) localización geográfica en tiempo real, 3) extracción de información de dispositivos electrónicos, y 4) escuchas.
- Las empresas telefónicas tienen una obligación jurídica para cooperar con las instancias de procuración de justicia, seguridad pública y seguridad

nacional para proveer la información aprobada por el órgano judicial relacionada con comunicaciones entre privados.

Capítulo 3.

- En la FGR las áreas relacionadas con las actividades sustantivas de las intervenciones son: la Fiscalía Especializada en materia de Delincuencia Organizada, la Agencia de Investigación Criminal y el Centro Federal de Inteligencia Criminal.
- En la GN las áreas involucradas en las intervenciones son: el Comandante General, la Jefatura General de Coordinación Policial, la Subjefatura de Investigación e Inteligencia, la Dirección General de Inteligencia y la Dirección de Vigilancia y Supervisión Interna.
- Ante la acción de inconstitucionalidad 62/2019 promovida por la CDNH, la SCJN validó diversos preceptos de la Ley de Guardia Nacional, entre ellos algunos relacionados con la posibilidad de solicitar a la autoridad judicial la intervención de comunicaciones para la prevención del delito.
- Existe poca información disponible sobre el funcionamiento del CNI, la SEDENA y la SEMAR con respecto a las intervenciones de comunicaciones. No obstante, se hizo un esfuerzo por indagar sobre las áreas responsables en fuentes abiertas.
- En el CNI sería la Coordinación General de Servicios Técnicos, particularmente con la Dirección de Intervenciones y la Dirección de Desarrollo Tecnológico.
- Entre 2016 y 2017, al Poder Judicial de la Federación habría autorizado más de 3 mil 800 solicitudes de intervenciones al CNI. Desde 2018 a 2021, no existen registros de solicitudes aprobadas para la institución.
- En SEDENA serían dos áreas las encargadas de las intervenciones: la Sección Segunda encargada de la Jefatura de Inteligencia y el Centro de Inteligencia Militar, ambas dependientes del Estado Mayor.
- En SEMAR sería la Unidad de Inteligencia Naval la encargada de realizar estas actividades.

- SEDENA y SEMAR carecen de un marco legal que dé certeza jurídica a los ciudadanos en intervención de comunicaciones privadas, específicamente no cuentan con atribuciones de investigación en procuración de justicia ni seguridad pública que justifiquen su realización en estos rubros. Es importante que el legislador colme este vacío jurídico.
- De acuerdo con medios de comunicación, de 2016 a 2021, en México, se tenían intervenidos más de 15 mil dispositivos telefónicos con la infección del *malware* Pegasus.
- Pegasus es un programa computacional que permite que el dispositivo se convierta en una herramienta de espionaje a control remoto. Es posible leer mensajes de texto, revisar fotos o conocer la ubicación en tiempo real, incluso se pueden activar las cámaras o los micrófonos sin que los usuarios lo detecten.
- Entre el 2011 y hasta 2013, la SEDENA, la SEMAR, la FGR y el CNI estarían involucrados en diferentes momentos en el uso de Pegasus. También existen otros tipos de tecnología para realizar un supuesto “espionaje” que serían utilizadas.
- La CIDH y la CNDH han hecho pronunciamiento relacionados con la urgencia de intensificar los esfuerzos para investigar el mal uso de estas tecnologías contra civiles y sobre la laxitud del marco jurídico.

Recomendaciones

Ahora bien, con las temáticas revisadas hasta el momento a lo largo del capitulado y como parte de la contribución de la investigación se formulan 11 recomendaciones en materia de legislación y otros temas generales sobre las intervenciones de comunicaciones privadas:

1. **Garantizar el derecho a la privacidad**. Como lo señala la organización R3D, se deben adoptar todas las medidas necesarias para respetar, proteger y garantizar el derecho a la privacidad y la libertad de expresión, el ejercicio

del periodismo, la defensa de los derechos humanos y la participación pública.[91]

2. **Legislación sobre aspectos fundamentales.** Si bien existe un marco jurídico desarrollado en materia de intervenciones, es necesario definir claramente en el marco legal de seguridad pública, seguridad nacional y procuración de justicia los conceptos de intervenciones, técnicas que se pueden realizar y, sobre todo, los alcances. Es decir, qué pueden y qué no pueden realizar las instituciones y autoridades en el marco de su competencia. La existencia de un marco jurídico laxo puede dar lugar a interpretaciones ambiguas para la acción institucional y, como consecuencia, la violación a los derechos humanos.
3. **Legislación sobre equipos tecnológicos**. Es un tema de primera importancia el emitir legislación en lo relacionado con la adquisición de este tipo de tecnología. Existe un vacío jurídico en cuanto a las reglas para la su obtención y operación. Prácticamente cualquier entidad pública o privada que tenga los recursos podría adquirir hipotéticamente estos dispositivos, lo cual representa un potencial riesgo para la privacidad de las personas y, en última instancia, para la democracia debido al posible espionaje.[92]
4. **Legislación sobre avances tecnológicos**. El marco legal debe integrar explícitamente las nuevas tecnologías y modalidades de comunicación. Los mensajes y llamadas por internet, así como diversas formas de comunicación a través de aplicaciones móviles y tecnologías subyacentes, son cada vez

[91] Red en Defensa de los Derechos Digitales, *LA CIDH MUESTRA PREOCUPACIÓN POR EL ESPIONAJE CON PEGASUS EN MÉXICO*, *Óp. Cit.*

[92] De hecho, la CNDH emitió la "Recomendación General 47/2022. Ausencia de regulación jurídica para la adquisición y uso de tecnologías para la vigilancia, intervención y recolección de datos de personas en territorio nacional: su impacto en la libertad de expresión, el derecho a defender Derechos Humanos y su vinculación al de deber de cuidado a cargo del Estado mexicano". En ésta señala que existe evidencia que agencias del gobierno mexicano han adquirido durante los últimos años *software* de espionaje, que tiene como objeto afectar el derecho a las comunicaciones privadas de periodistas, comunicadores y personas defensoras de derechos humanos. Por tanto, se realiza el llamado para atender la problemática que deriva de la existencia de normas generales, ambiguas y/o deficientes, que propician la posibilidad de injerencias ilegales y arbitrarias en la vida privada de cualquier persona que se encuentre en el territorio nacional. *Ver*. Comisión Nacional de Derechos Humanos, "CNDH emite Recomendación General a autoridades del Estado mexicano por el caso de espionaje y su impacto en la libertad de expresión relacionado con el software Pegasus", *Óp. Cit.*

más comunes, por lo que es necesario que el marco jurídico se adecúe a esta nueva realidad.

5. **Instrumentos de derecho público internacional**. Es necesario crear y actualizar acuerdos binacionales con los países con los que se tiene la mayor cooperación en seguridad pública, seguridad nacional y procuración de justicia para la asistencia jurídica y para la persecución del delito a nivel supranacional. De la misma forma, sería deseable la creación de acuerdos para la conformación de instrumentos jurídicos regionales tendientes a la cooperación en materia de intervención de comunicaciones privadas, mismos que en la actualidad no existen.
6. **Legislación en seguridad pública y nacional.** Hoy por hoy el ámbito de procuración de justicia tiene el marco jurídico más desarrollado para la solicitud de las intervenciones. Dado que se requiere dar certeza jurídica al imputado en el sistema de justicia penal acusatorio, las reglas para la solicitud e implementación de las intervenciones son globalmente adecuadas. En contraste, en los ámbitos de seguridad pública y seguridad nacional se carece de un marco legal desarrollado para la implementación de las intervenciones por parte de las instituciones responsables. De suerte que es necesario que se mejore la calidad de la legislación en la materia.
7. **Legislación para las Fuerzas Armadas**. De manera clara y directa: no existe legislación actual que regule la actuación de SEDENA y SEMAR en la realización de las intervenciones de comunicaciones privadas en el ámbito del fuero civil. Éste es uno de los principales hallazgos de la investigación. Derivado de la revisión de fuentes abiertas, es claro que las dependencias han realizado este tipo de actividades durante los últimos años pero carecen de cualquier marco jurídico. Esto, por decir lo menos, es preocupante. Al igual que la FGR y la GN, las Fuerzas Armadas deberían tener un control constitucional para la realización de las intervenciones.
8. **Fiscalización**. En 2024, no existe un organismo que tenga capacidades desarrolladas para la supervisión de las intervenciones en entidades de la administración pública federal o local. Debería ser fundamental dotar a una

o más instituciones externas e imparciales de las capacidades para supervisar las intervenciones de comunicaciones. Dentro de las dependencias que podrían realizar esta función se encuentra la Auditoría Superior de la Federación, el Sistema Nacional Anticorrupción o la CNDH.

9. **Transparencia**. Si bien, en términos de la Ley General en la materia, la FGR, la GN, la SEDENA, la SEMAR y el CNI deben emitir información estadística en materia de intervención de comunicaciones y debe estar disponible en la Plataforma Nacional de Transparencia[93], ésta es por lo general escasa, de poca calidad y no permite profundizar en la comprensión de los datos. Es necesario que exista una mayor apertura por parte de las dependencias para desclasificar información no sensible después de cierto tiempo, sin ahondar en las investigaciones específicas y sin exponer datos personales. Esto con la finalidad que la sociedad civil cuente con una mayor claridad de quiénes, cuándo y por qué realizan las intervenciones y cómo se justifica su actuar.
10. **Estudios especializados**. De manera similar a lo estipulado legalmente con el IFETEL, es necesario que dependencias de la administración pública desarrollen estudios especializados y soluciones tecnológicas que permitan inhibir y combatir la realización de delitos vinculados con intervenciones de comunicaciones privadas, principalmente en materia de seguridad pública y seguridad nacional.
11. **Investigación penal sobre programas de espionaje**. En los últimos años, se tornó esencial el investigar de forma completa, exhaustiva e imparcial la adquisición y el uso de los diferentes programas que se utilizan con fines de espionaje (incluyendo Pegasus) y sancionar penalmente a quienes resulten responsables dentro del ámbito público o privado. Esto debería ser una tarea del Estado mexicano dado su gravedad e importancia con la intención de inhibir conductas similares hacia el futuro.[94]

---

[93] Ver. Plataforma Nacional de Transparencia, disponible en: https://consultapublicamx.plataformadetransparencia.org.mx/vut-web/faces/view/consultaPublica.xhtml#inicio [consulta: diciembre, 2023]

[94] Red en Defensa de los Derechos Digitales, *LA CIDH MUESTRA PREOCUPACIÓN POR EL ESPIONAJE CON PEGASUS EN MÉXICO*, *Óp. Cit.*

Lo señalado a lo largo de la tesina no tiene la finalidad de esgrimir críticas o de resaltar la mala acción de las instituciones mexicanas, al contrario, se trata de planteamientos propositivos que podrían retomarse con la intención de fortalecer el marco jurídico y de acción en materia de intervención de comunicaciones privadas.

Es importante reconocer que quedan abiertas dos líneas de investigación que implican la realización de documentos especializados independientes por su profundidad y complejidad, que fueron abordadas brevemente en esta tesina y de las cuales no es posible obtener conclusiones en este momento.

Primero, las intervenciones en las Fiscalías y Secretarías de Seguridad de las 32 entidades federativas que tienen una dinámica propia y que, al ser revisadas, probablemente se encuentren inconsistencias jurídicas que deban reformarse. En ellas se cuenta con áreas, personal y equipo especializado que es necesario fiscalizar y asegurarse que no trabajen más allá de los límites que explícitamente impone la ley.

Segundo, como parte de la investigación, se identificó que hay un enorme “mercado negro” para la compraventa de las diferentes modalidades de intervenciones de comunicaciones privadas. Es decir, se comercializan de manera ilegal datos conservados, localizaciones geográficas en tiempo real, extracción de información, escuchas y otras actividades relacionadas. Por lo tanto, se debe prestar atención urgente a esta situación donde podrían estar involucradas empresas de telecomunicaciones, empresas privadas, particulares, autoridades y otros actores relevantes. Como consecuencia, es necesario duplicar esfuerzos para emitir legislación e impulsar mecanismos institucionales para disminuir el mercado negro anteriormente descrito.

Para cerrar la investigación es preciso indicar que, como se sostuvo a lo largo de la tesina, las intervenciones de comunicaciones privadas son técnicas fundamentales para las instituciones de seguridad pública, seguridad nacional y procuración de justicia. Proveen a las autoridades de herramientas valiosas para la prevención, investigación y persecución del delito, por tanto es necesario reforzar el andamiaje

jurídico en un marco de respeto irrestricto al estado de derecho y a los derechos humanos.

Bibliografía

—Asamblea General de las Naciones Unidas, *Declaración Universal de Derechos Humanos*, 10 de diciembre de 1948, dirección URL: https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf [consulta: septiembre, 2023].

—Asamblea General de las Naciones Unidas, Pacto Internacional de Derechos Civiles y Políticos, diciembre de 1996, dirección URL: https://www.ohchr.org/sites/default/files/ccpr_SP.pdf [consulta: septiembre, 2023].

—Badillo, Miguel, "La nueva estructura y los salarios del Centro Nacional de Inteligencia", en *Contralínea*, México, 06 de mayo de 2023, dirección URL: https://contralinea.com.mx/interno/semana/la-nueva-estructura-y-los-salarios-del-centro-nacional-de-inteligencia/ [consulta: diciembre, 2023].

—Cabrera, David, "GN solicitó 67 mdp para intervenir comunicaciones de 500 objetivos", en *La Otra Opinión, México – Ricardo Alemán*, 08 de septiembre de 2022, dirección URL: https://laotraopinion.com.mx/gn-solicito-67-mdp-para-intervenir-comunicaciones-de-500-objetivos/ [consulta: diciembre, 2023].

—Camacho, Zózimo, "Cisen: 11 años de comunicaciones intervenidas", en *Contralínea*, México, 11 de octubre de 2017, dirección URL: https://contralinea.com.mx/noticias/cisen-11-anos-comunicaciones-intervenidas/ [consulta: diciembre, 2023].

—Castillo, Gustavo y Murillo, Eduardo, "Al llegar AMLO cesaron peticiones de intervención telefónica", en *La Jornada*, México, 22 de julio de 2021, dirección URL: https://www.jornada.com.mx/notas/2021/07/22/politica/al-llegar-amlo-cesaron-peticiones-de-intervencion-telefonica/ [consulta: diciembre, 2023].

—Comisión Nacional de Derechos Humanos, "CNDH emite Recomendación General a autoridades del Estado mexicano por el caso de espionaje y su impacto en la libertad de expresión relacionado con el software Pegasus", México, 26 de mayo de 2022, dirección URL: https://www.cndh.org.mx/sites/default/files/documentos/2022-05/COM_2022_154.pdf [consulta: diciembre, 2023].

—Comisión Nacional de los Derechos Humanos, *Demanda de acción de inconstitucionalidad, promovida por la CNDH*, México, 26 de junio de 2019, dirección

URL: https://www.cndh.org.mx/sites/default/files/documentos/2019-07/Acc_Inc_2019_62.pdf [consulta: diciembre, 2023].

—Congreso de la Unión, *Código Militar de Procedimientos Penales*, México, publicada en el Diario Oficial de la Federación el 16 de mayo de 2016, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/CMPP.pdf [consulta: julio, 2023].

—Congreso de la Unión, *Código Nacional de Procedimientos Penales*, México, publicada en el Diario Oficial de la Federación el 05 de marzo de 2014, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf [consulta: julio, 2023].

—Congreso de la Unión, *Código Penal Federal*, México, publicada en el Diario Oficial de la Federación el 14 de agosto de 1931, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf [consulta: mayo, 2023].

—Congreso de la Unión, *Constitución Política de los Estados Unidos Mexicanos*, México, publicada en el Diario Oficial de la Federación el 05 de febrero de 1917, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf [consulta: julio, 2023].

—Congreso de la Unión, *Ley de la Guardia Nacional*, México, publicada en el Diario Oficial de la Federación el 27 de mayo de 2019, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf [consulta: julio, 2023].

—Congreso de la Unión, *Ley de Seguridad Nacional*, México, publicada en el Diario Oficial de la Federación el 31 de enero de 2005, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf [consulta: julio, 2023].

—Congreso de la Unión, *Ley Federal contra la Delincuencia Organizada*, México, publicada en el Diario Oficial de la Federación el 07 de noviembre de 1996, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFCDO.pdf [consulta: julio, 2023].

—Congreso de la Unión, *Ley Federal de Telecomunicaciones y Radiodifusión*, México, publicada en el Diario Oficial de la Federación el 14 de julio de 2014, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf [consulta: octubre de 2023].

—Congreso de la Unión, *Ley Orgánica del Poder Judicial de la Federación*, México, publicada en el Diario Oficial de la Federación el 07 de junio de 2021, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LOPJF.pdf [consulta: agosto, 2023].

—Congreso de la Unión, *Reglamento de la Ley de la Guardia Nacional*, México, publicada en el Diario Oficial de la Federación el 29 de junio de 2019, dirección URL: https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGN_111220.pdf

—Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, Bruselas, noviembre de 2021, dirección URL: https://rm.coe.int/16802fa403 [consulta: septiembre, 2023].

—Consejo de la Judicatura Federal, *Acuerdo General 12/2021, del Pleno del Consejo de la Judicatura Federal, que Reforma el Artículo 13, del similar 3/2017 del Pleno del Consejo de la Judicatura Federal por el que se Crea el Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones; en Relación con su Periodo Vacacional*, publicado el 20 de septiembre de 2021, dirección URL: https://www.google.com/search?q=ACUERDO+GENERAL+12%2F2021%2C+DEL+PLENO+DEL+CONSEJO+DE+LA+JUDICATURA+FEDERAL%2C+QUE+REFORMA+EL+ART%C3%8DCULO+13%2C+DEL+SIMILAR+3%2F2017+DEL+PLENO+DEL+CONSEJO+DE+LA+JUDICATURA+FEDERAL+POR+EL+QUE+SE+CREA+EL+CENTRO+NACIONAL+DE+JUSTICIA+ESPECIALIZADO+EN+CONTROL+DE+T%C3%89CNICAS+DE+INVESTIGACI%C3%93N%2C+ARRAIGO+E+INTERVENCI%C3%93N+DE+COMUNICACIONES%3B+EN+RELACI%C3%93N+CON+SU+PERIODO+VACACIONAL.&oq=ACUERDO+GENERAL+12%2F2021%2C+DEL+PLENO+DEL+CONSEJO+DE+LA+JUDICATURA+FEDERAL%2C+QUE+REFORMA+EL+ART%C3%8DCULO+13%2C+DEL+SIMILAR+3%2F2017+DEL+PLENO+DEL+CONSEJO+DE+LA+JUDICATURA+FEDERAL+POR+EL+QUE+SE+CREA+EL+CENTRO+NACIONAL+DE+JUSTICIA+ESPECIALIZADO+EN+CONTROL+DE+T%C3%89CNICAS+DE+INVESTIGACI%C3%93N%2C+ARRAIGO+E+INTERVENCI%C3%93N+DE+COMUNICACIONES%3B+EN+RELACI%C3%93N+CON+SU+PERIODO+VACACIONAL.&aqs=chrome..69i57.598j0j7&sourceid=chrome&ie=UTF-8 [consulta: agosto, 2023].

—Consejo de la Judicatura Federal, *Acuerdo General 3/2017 del Pleno del Consejo de la Judicatura Federal, por el que se crea el Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones*, publicado en el Diario Oficial de la Federación el 15 de mayo de 2017, dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5482579&fecha=15/05/2017#gsc.tab=0 [consulta: agosto, 2023].

—Consejo de la Judicatura Federal, *Acuerdo General 5/2019 del Pleno del Consejo de la Judicatura Federal, que reforma los artículos 14 y 19 del Diverso 3/2017, por el que se crea el Centro Nacional de Justicia Especializado en Control de Técnicas de Investigación, Arraigo e Intervención de Comunicaciones*, publicado en el Diario Oficial de la Federación el 21 de mayo de 2019, dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5560782&fecha=21/05/2019#gsc.tab=0 [consulta: agosto, 2023].

—Fiscalía General de la República, *ACUERDO POR EL QUE SE DELEGAN DIVERSAS FACULTADES EN LAS PERSONAS AGENTES DEL MINISTERIO PÚBLICO DE LA FEDERACIÓN*, México, 06 de diciembre de 2023, dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5710651&fecha=06/12/2023#gsc.tab=0 [consulta: diciembre, 2023].

—Fiscalía General de la República. *ACUERDO A/001/2023 por el que se emite el Manual de Organización y Procedimientos de la Fiscalía General de la República*, México, publicado en el Diario Oficial de la Federación el 09 de octubre de 2023, dirección URL: https://sidof.segob.gob.mx/notas/5704316 [consulta: noviembre, 2023].

—Gallegos, Zorayda, “La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles”, en El País, México, 14 de abril de 2021, dirección URL: https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html [consulta: diciembre, 2023] y Red en Defensa de los Derechos Digitales, “#FISCALÍAESPÍA: LA FGR ADQUIRIÓ EQUIPO CAPAZ DE ESPIAR ILEGALMENTE A TODOS LOS USUARIOS DE INTERNET EN MÉXICO”, México, 14 de abril de 2021, dirección URL:

https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/ [consulta: diciembre, 2023].

—Gobierno de la República, *Declaración Universal. Versión Comentada*, Guatemala, 2011, dirección URL: https://www.corteidh.or.cr/tablas/28141.pdf [consulta: septiembre, 2023].

—Gobierno de la República, *Tratado de Cooperación entre los Estados Unidos Mexicanos y los Estados Unidos de América sobre Asistencia Jurídica Mutua*, México, Ciudad de México, diciembre de 1987, dirección URL: https://aplicaciones.sre.gob.mx/tratados/ARCHIVOS/EUA-ASISTENCIA%20JURIDICA.pdf [consulta: septiembre, 2023].

https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGN_111220.pdf [consulta: noviembre, 2023].

—Instituto Federal de Telecomunicaciones, *Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996*, México, publicada en el Diario Oficial de la Federación, el 02 de diciembre de 2015, dirección URL: https://dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015&print=true [consulta: octubre de 2023].

—Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *INAI instruye a FGR informar sobre intervención de comunicaciones privadas, de 2018 a 2020*, México, 08 de agosto de 2021, dirección URL: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-066-21.pdf [consulta: diciembre, 2023].

—Mendoza Cortés, Paloma, “Inteligencia y contrainteligencia militar frente a fallos y desafíos. El caso de Culiacán, México (2019)”, en *Revista Latinoamericana de Estudios de Seguridad*, N° 26, FLACSO Ecuador, enero de 2020.

—Microsoft, ¿Qué es el malware?, dirección URL: https://www.microsoft.com/es-mx/security/business/security-101/what-is-malware [consulta: diciembre, 2023].

—Monroy, Jorge, “15,000 números telefónicos de México fueron detectados en lista de malware de espionaje Pegasus: The Guardian”, en *El Economista*, México, 18 de julio de 2021, dirección URL: https://www.eleconomista.com.mx/politica/15000-numeros-telefonicos-de-Mexico-fueron-detectados-en-lista-de-malware-de-espionaje-Pegasus-The-Guardian-20210718-0025.html [consulta: diciembre, 2023] y Garduño, Mónica, “Así logró el software Pegasus espiar a 25 periodistas mexicanos”, en *Forbes*, México, 21 de julio de 2021, dirección URL: https://www.forbes.com.mx/tecnologia-asi-software-pegasus-espiar-25-periodistas-mexicanos/ [consulta: diciembre, 2023].

—Organización de Estados Americanos, *Convención Americana Sobre Derechos Humanos*, mayo de 1991, dirección URL: https://www.cndh.org.mx/sites/default/files/doc/Programas/TrataPersonas/MarcoNormativoTrata/InsInternacionales/Regionales/Convencion_ADH.pdf [consulta: septiembre, 2023].

—Organización de Estados Americanos, *Convención Interamericana contra la Corrupción*, Venezuela, marzo de 1997, dirección URL: https://www.oas.org/es/sla/ddi/docs/tratados_multilaterales_interamericanos_b-58_contra_corrupcion.pdf [consulta: septiembre, 2023].

—Plataforma Nacional de Transparencia. *Intervención de comunicaciones privadas*, actualizado a diciembre de 2023, dirección URL: https://consultapublicamx.plataformadetransparencia.org.mx/vut-web/faces/view/consultaPublica.xhtml#tarjetaInformativa [consulta: diciembre, 2023].

—Real Academia de la Lengua Española, Definición: espionaje, España, dirección URL: https://dle.rae.es/espionaje [consulta: diciembre, 2023].

—Red en Defensa de los Derechos Digitales, #EJÉRCITOESPÍA: NUEVOS CASOS DE ESPIONAJE CON PEGASUS EN MÉXICO NO DEBEN QUEDAR EN LA IMPUNIDAD, México, 03 de octubre de 2022, dirección URL: https://r3d.mx/2022/10/03/nuevos-casos-de-espionaje-con-pegasus-en-mexico-no-deben-quedar-en-la-impunidad/ [consulta: diciembre, 2023].

—Red en Defensa de los Derechos Digitales, *CITIZEN LAB REVELA USO DE SOFTWARE ESPÍA DE CIRCLES, EMPRESA VINCULADA CON NSO GROUP, EN MÉXICO*, México, 01 de diciembre de 2020, dirección URL: https://r3d.mx/2020/12/01/citizen-lab-revela-uso-de-software-espia-de-circles-empresa-vinculada-con-nso-group-en-mexico/ [consulta: diciembre, 2023].

—Red en Defensa de los Derechos Digitales, *CORTE INVALIDA INTERVENCIÓN DE COMUNICACIONES PRIVADAS POR MILITARES SIN AUTORIZACIÓN DE UN JUEZ CIVIL*, México, 17 de abril de 2023, dirección IRL: https://r3d.mx/2023/04/17/corte-invalida-intervencion-de-comunicaciones-privadas-por-militares-sin-autorizacion-de-un-juez-civil/ [consulta: diciembre, 2023]

—Red en Defensa de los Derechos Digitales, *EMPRESARIO SE DECLARA CULPABLE DE VENDER EQUIPO DE ESPIONAJE EN MÉXICO A SABIENDAS DE SU USO ILEGAL*, México, 17 de febrero de 2022, dirección URL: https://r3d.mx/2022/02/17/empresario-se-declara-culpable-de-vender-equipo-de-espionaje-en-mexico-a-sabiendas-de-su-uso-ilegal/ [consulta: diciembre, 2023].

—Red en Defensa de los Derechos Digitales, *FISCALÍA DE CDMX ACCEDIÓ A REGISTROS TELEFÓNICOS PARA ESPIAR A FIGURAS POLÍTICAS*, México, 09 de noviembre de 2023, dirección URL: https://r3d.mx/2023/11/09/fiscalia-de-cdmx-accedio-a-registros-telefonicos-para-espiar-a-figuras-politicas/ [consulta: diciembre, 2023].

—Red en Defensa de los Derechos Digitales, *LA CIDH MUESTRA PREOCUPACIÓN POR EL ESPIONAJE CON PEGASUS EN MÉXICO*, México, 02 de junio de 2023, dirección URL: https://r3d.mx/2023/06/02/la-cidh-muestra-preocupacion-por-el-espionaje-con-pegasus-en-mexico/ [consulta: diciembre, 2023].

—Red en Defensa de los Derechos Digitales, *LA SEDENA ES ACTUALMENTE EL ÚNICO OPERADOR DE PEGASUS EN MÉXICO, REVELA NYT*, México, 19 de abril de 2023, dirección URL: https://r3d.mx/2023/04/19/la-sedena-es-actualmente-el-unico-operador-de-pegasus-en-mexico-revela-nyt/ [consulta: diciembre, 2023].

—Red en Defensa de los Derechos Digitales, *LO QUE SABEMOS DE LAS AUTORIDADES QUE ADQUIRIERON PEGASUS EN MÉXICO*, México, 23 de julio

de 2021, dirección URL: https://r3d.mx/2021/07/23/autoridades-pegasus-mexico/ [consulta: diciembre, 2023].

—Red en Defensa de los Derechos Digitales, *MÉXICO YA NO PODRÍA IMPORTAR TECNOLOGÍAS DE VIGILANCIA DE EMPRESAS ISRAELÍES*, México, 25 de noviembre de 2025, dirección URL: https://r3d.mx/2021/11/25/mexico-ya-no-podria-importar-tecnologias-de-vigilancia-de-empresas-de-israel/ [consulta: diciembre, 2023].

—Redacción, "Guardia Nacional pidió 67.1 mdp para equipo de intervención de comunicaciones", en *Aristegui Noticias*, México, 07 de septiembre de 2022, dirección URL: https://aristeguinoticias.com/0709/mexico/guardia-nacional-pide-dinero-para-intervenir-comunicaciones-de-500-objetivos/ [consulta: diciembre, 2023].

—Secretaría de Marina – Armada de México, *ACUERDO Secretarial número 172, por el que se expide el Manual de Organización General de la Secretaría de Marina*, México, publicado en el Diario Oficial de la Federación el 29 de julio de 2016, dirección URL: https://dof.gob.mx/nota_detalle.php?codigo=5446206&fecha=29/07/2016#gsc.tab=0 [consulta: diciembre, 2023].

—Secretaría de Seguridad y Protección Ciudadana, *ACUERDO por el que se crea la Subjefatura de Investigación e Inteligencia de la Guardia Nacional*, México, 28 de septiembre de 2023, dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5703227&fecha=28/09/2023#gsc.tab=0 [consulta: noviembre, 2023].

—Senado de la República, *PROPOSICIÓN CON PUNTO DE ACUERDO DE URGENTE Y OBVIA RESOLUCIÓN, POR EL QUE SE SOLICITA AL EJECUTIVO FEDERAL REMITA A ESTA SOBERANIA Y SE HAGA PÚBLICA LA INFORMACIÓN RELATIVA AL ESPIONAJE E INTERVENCION DE COMUNICACIONES PRIVADAS A TRAVÉS DE LA APLICACIÓN PEGASUS DE LA FIRMA TECNOLÓGICA ISRAELI NSO GROUP CONTRATADA POR EL GOBIERNO FEDERAL Y DE OTROS MECANISMOS DE INTERVENCIÓN ILEGAL DE COMUNICACIONES PRIVADAS, Y A LA FISCALIA GENERAL DE LA REPÚBLICA*

PARA QUE INICIE UNA INVESTIGACIÓN, SE FINQUEN RESPONSABILIDADES Y SE INICIEN LOS PROCESOS JUDICIALES CORRESPONDIENTES, México, 21 de julio de 2021, dirección URL: https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-07-29-1/assets/documentos/123-PA_Aplicacion-PEGASUS.pdf [consulta: diciembre, 2023].

—Suprema Corte de Justicia de la Nación, *2a. CLX/2000*, México, novena época, Segunda Sala de la Suprema Corte de Justicia de la Nación: publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XII, Diciembre de 2000, página 428, dirección URL: https://sjf2.scjn.gob.mx/detalle/tesis/190652 [consulta: octubre, 2023].

—Suprema Corte de Justicia de la Nación, *P. XXXI/2008*, México, novena época, pleno de la Suprema Corte de Justicia de la Nación: publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XXVII, Abril de 2008, página 5, dirección URL: https://sjf2.scjn.gob.mx/detalle/tesis/169884 [consulta: octubre, 2023].

—Suprema Corte de Justicia de la Nación, *P. XXXIII/2008*, México, novena época, pleno de la Suprema Corte de Justicia de la Nación: publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XXVII, Abril de 2008, página 6, dirección URL: https://sjf2.scjn.gob.mx/detalle/tesis/169859 [consulta: octubre, 2023].

—Suprema Corte de Justicia de la Nación, SCJN ANALIZA DIVERSAS DISPOSICIONES DE LA LEY DE LA GUARDIA NACIONAL, México, 24 de abril de 2023, dirección URL: https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=7333 [consulta: diciembre, 2023].

—Suprema Corte de Justicia de la Nación, *Síntesis informativa*, México, 18 de abril de 2023, dirección URL: https://www.scjn.gob.mx/sites/default/files/sintesis-informativa/2023-04/S%C3%ADntesisPDF-18abril2023.pdf [consulta: diciembre, 2023].

—Tourliere, Mathieu, “Centro Militar de Inteligencia, el búnker de la 4T para espiar”, en *Revista Proceso*, México, 11 de marzo de 2023, dirección URL: https://www.proceso.com.mx/reportajes/2023/3/11/centro-militar-de-inteligencia-el-bunker-de-la-4t-para-espiar-303474.html [consulta: diciembre, 2023].

—Vega, Carlos, “Guardia Nacional gestiona 846 mdp para inteligencia anticrimen”, en *Milenio*, México, 28 de octubre de 2022, dirección URL: https://www.milenio.com/policia/guardia-nacional-gestiona-846-mdp-inteligencia-anticrimen [consulta: diciembre, 2023].