DECRETO POR EL QUE SE REFORMAN, DEROGAN Y ADICIONAN DIVERSAS DISPOSICIONES EN MATERIA DE INTERVENCIÓN DE COMUNICACIONES PRIVADAS Y VIGILANCIA GUBERNAMENTAL

Las que suscribimos —--, en ejercicio de la facultad que nos otorga el artículo 71, fracción VI, de la Constitución Política de los Estados Unidos Mexicanos y con fundamento en los artículos 58 y 61 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, presentamos ante esta Honorable Cámara de Diputados del Congreso de la Unión la propuesta de **DECRETO POR EL QUE SE REFORMAN, DEROGAN Y ADICIONAN DIVERSAS DISPOSICIONES EN MATERIA DE INTERVENCIÓN DE COMUNICACIONES PRIVADAS Y VIGILANCIA GUBERNAMENTAL**, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

En el Informe "El Estado de la Vigilancia"[1], la organización Red en Defensa de los Derechos Digitales (R3D) realiza un análisis de la regulación y la práctica de la vigilancia de comunicaciones en México, contrastada con los estándares internacionales en materia de protección de derechos humanos aplicables a esta actividad. Con base en dicho informe se presenta un diagnóstico que resume las deficiencias, desafíos y problemas que requieren ser corregidos para revertir la impunidad con que la vigilancia de comunicaciones es abusada en México.

DIAGNÓSTICO

A. Incertidumbre jurídica

Como es advertido en el Capítulo Segundo del Informe citado, la regulación de la vigilancia de comunicaciones posee diversas deficiencias que producen incertidumbre jurídica.

a. Sobre las autoridades facultadas

A pesar de que la Constitución, las leyes y la interpretación de la SCJN[2] únicamente reconocen como autoridades facultadas expresamente para llevar a cabo medidas de vigilancia de comunicaciones a la Guardia Nacional, el Centro Nacional de Inteligencia, la Fiscalía General de la República, las 32 fiscalías estatales y la Fiscalía General de Justicia Militar, en el marco de sus respectivas competencias, persisten autoridades federales y locales que derivan facultades para vigilancia de comunicaciones, como la geolocalización en tiempo real o el

[1] R3D. *El Estado de la Vigilancia.* Enero de 2025. Disponible en: https://r3d.mx/publicaciones/

[2] Ver por ejemplo: **Amparo en Revisión 964/2015**. Sentencia de 4 de mayo de 2016, resuelta por unanimidad de cinco votos de los señores Ministros: Eduardo Medina Mora I., Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Presidente Alberto Pérez Dayán (ponente). Los señores Ministros José Fernando Franco González Salas y Margarita Beatriz Luna Ramos emitieron su voto en contra de consideraciones, pp. 63 a 64.

acceso a datos conservados por empresas de telecomunicaciones, de normas vagas e imprecisas o las llevan a cabo sin fundamentación alguna.

Esta incertidumbre jurídica no solamente aumenta los riesgos para las personas potencialmente vigiladas ilegalmente en perjuicio de su privacidad y seguridad, sino que puede conllevar responsabilidad legal para las empresas que colaboran en el despliegue de las medidas de vigilancia, e incluso puede poner en riesgo la validez jurídica de actuaciones por parte de autoridades, lo cual puede ocasionar perjuicios al interés público.

b. Sobre los requisitos de procedencia material

La claridad y precisión de los requisitos de procedencia material para llevar a cabo medidas de vigilancia es variable dentro del marco jurídico mexicano. Por ejemplo, a pesar de que la Ley de la Guardia Nacional (LGN) requiere que se constate "la existencia de indicios suficientes que acrediten que se está organizando la comisión de delitos" enlistados en el artículo 103 de la LGN, otros ordenamientos poseen requisitos de procedencia amplios y vagos. Resalta la Ley de Seguridad Nacional (LSN), la cual permite medidas como la intervención de comunicaciones cuando a juicio del CNI existan "amenazas a la seguridad nacional", las cuales son definidas de manera amplia y vaga en el artículo 5 de la LSN.

Igualmente, en algunos casos, el Código Nacional de Procedimientos Penales (CNPP) faculta a las fiscalías a llevar a cabo medidas de vigilancia cuando el propio Ministerio Público las considere necesarias. La constatación de la necesidad de las medidas debe ser apreciada por el juez de control federal competente a partir de indicios objetivos presentados por la autoridad que solicita autorización, sin embargo, la redacción defiere en exceso a la propia autoridad para justificar la pertinencia de una medida de vigilancia.

c. Sobre el control judicial previo o inmediato

Reformas al CNPP y algunos precedentes judiciales han establecido con mayor claridad la necesidad de control judicial previo, como regla general, para llevar a cabo medidas de vigilancia como el acceso a datos conservados por empresas de telecomunicaciones o la geolocalización en tiempo real. Sin embargo, persisten incertidumbre jurídica respecto del control judicial de las medidas de vigilancia.

Por ejemplo el mecanismo excepcional establecido en el artículo 303 del CNPP, por el que las fiscalías pueden solicitar el acceso a datos conservados o la geolocalización en tiempo real a empresas de telecomunicaciones sin obtener previamente una autorización judicial, sino con la carga de solicitar la ratificación de la medida dentro de las 48 horas posteriores a la solicitud original, ha provocado que la excepción se convierta en la regla general y que un número importante de solicitudes realizadas bajo el mecanismo excepcional no sean ratificadas por la autoridad judicial federal, o inclusive ni siquiera sean sometidas a dicha ratificación, permitiendo así que autoridades invadan la privacidad de personas usuarias de telecomunicaciones ilegal e impunemente, sin que la persona afectada o un juez siquiera tengan conocimiento de ello.

Por otro lado, si bien precedentes recientes de la SCJN han establecido con claridad que la autoridad judicial competente para evaluar las solicitudes de autorización para la intervención de comunicaciones privadas, el acceso a datos conservados o la geolocalización en tiempo real es la autoridad judicial federal[3], autoridades persisten en pretender que autoridades judiciales locales puedan tener competencia para autorizar dichas medidas de vigilancia.

Peor aún, diversas autoridades parecen interpretar que el requisito de autorización judicial previa resulta únicamente aplicable a medidas de vigilancia que requieren la colaboración de terceros, como empresas de telecomunicaciones o proveedores de servicios, aplicaciones y contenidos en Internet, y no así cuando las autoridades despliegan medidas de vigilancia de manera autónoma, por ejemplo a través de tecnologías de geolocalización como aquéllas que explotan las vulnerabilidades en el protocolo SS7 o incluso medidas de vigilancia masiva como las antenas falsas o la vigilancia masiva delegada a particulares con herramientas como *Echo*.

La elusión del control judicial a las medidas de vigilancia fomenta los abusos, impiden la detección de los mismos y permiten la impunidad que fomenta su repetición crónica. Por ello resulta necesario que el marco jurídico detalle con claridad la necesidad del control judicial federal previo o inmediato de todas las medidas de vigilancia reconocidas por el marco jurídico mexicano.

d. Sobre las formas de vigilancia

La proliferación de tecnologías de vigilancia masiva, como las antenas falsas o el outsourcing de vigilancia masiva, así como las tecnologías de vigilancia focalizada altamente invasiva y elusiva como el *spyware*, es indicativa de la poca claridad y precisión sobre las métodos de vigilancia que pueden considerarse compatibles con las normas de derechos humanos reconocidas en la Constitución.

Las normas que regulan la vigilancia en el marco jurídico mexicano fueron diseñadas pensando en tecnologías de intervención telefónica y otras formas de vigilancia focalizada que requerían la colaboración de particulares, especialmente empresas de telecomunicaciones. Los métodos tradicionales de vigilancia de comunicaciones ofrecían considerablemente menos información de las personas vigiladas y producían ineludiblemente testigos en las empresas de telecomunicaciones que colaboraban con dicha vigilancia, las cuales —en teoría— podrían resultar menos propensas a colaborar con intervenciones ilegales, es decir, aquéllas no autorizadas por un juez competente.

Sin embargo, tecnologías de *spyware* como *Pegasus* ofrecen una cantidad de información que no se limita a las conversaciones telefónicas de la persona vigilada, sino que permiten el

[3] Plenos Regionales. Tesis PR.P.CN. J/23 P (11a.) Gaceta del Semanario Judicial de la Federación. Libro 33, Enero de 2024, Tomo IV, página 3989. Registro digital: 2028011; y SCJN. Primera Sala. Tesis 1a. VI/2024 (11a.) Gaceta del Semanario Judicial de la Federación. Libro 37, Mayo de 2024, Tomo II, página 2250. Registro digital: 2028870.

acceso a información como contactos, fotografías, videos, archivos, mensajes de texto, geolocalización, contraseñas, historial de navegación, entre otra información que permite dibujar un panorama más completo de la vida privada de la persona vigilada, lo cual constituye una invasión intensa y sin paralelo a la intercepción telefónica tradicional.

Además, el hecho de que para ser desplegadas dichas tecnologías no requieren la colaboración de terceros, sino que son utilizadas de manera autónoma por la autoridad atacante, añadido a las características antiforenses y antidetección, implica un enorme desafío para evitar su utilización ilegal. Por lo que resulta poco sensato pretender que el marco jurídico actual sea capaz de asegurar su utilización racional o incluso la posibilidad de que dichas tecnologías puedan siquiera ser compatibles con los principios de necesidad y proporcionalidad.

Igualmente, además de que del marco constitucional y convencional se desprende la necesidad de que las medidas de vigilancia de comunicaciones se encuentren focalizadas a personas específicas, la proliferación y uso cotidiano de tecnologías de vigilancia masiva indican que el marco jurídico actual no ha ofrecido claridad suficiente para inhibir la adquisición y uso de dichas tecnologías de vigilancia.

B. Irregularidades y corrupción en la adquisición de tecnologías de vigilancia

Los procesos de contratación de equipos y sistemas para la vigilancia de comunicaciones se han distinguido por la opacidad, discrecionalidad y por la ausencia de regulación y controles adecuados para inhibir la corrupción, la vigilancia ilegal y la impunidad.

Dentro de las principales irregularidades respecto de los procesos de contratación de equipos y sistemas para la vigilancia destacan las siguientes:

a. Discrecionalidad y adjudicación a empresas con irregularidades

Prácticamente la totalidad de las contrataciones relacionadas a equipos o sistemas para la vigilancia de comunicaciones que han sido documentadas se han realizado mediante adjudicación directa, lo cual fomenta la discrecionalidad en la selección de empresas contratadas y la opacidad de las mismas.

Derivado de la opacidad y discrecionalidad con la que frecuentemente se han llevado a cabo los procesos de contratación relacionados a equipos y sistemas de vigilancia, así como de la inexistencia de regulación y el establecimiento de requisitos para el ofrecimiento de este tipo de herramientas, se han detectado procesos de contratación en los que la empresa contratada no posee antecedentes o experiencia en la materia o incluso posee irregularidades en su constitución o domicilio legal.

Es el caso de la empresa Grupo Tech Bull, la cual contrató con la PGR la venta de equipo y licencias para la operación del sistema *Pegasus* desarrollado por la empresa israelí NSO

Group. Como ha sido documentado, dicha empresa no poseía antecedentes o experiencia en la materia y no resulta conocida alguna contratación posterior. Además, el socio y administrador único de la empresa desconocía dicha contratación y las operaciones de la empresa y el domicilio legal de la misma no albergaba oficinas o trabajadores de la misma.

Resulta adicionalmente irregular que los procesos de renovación de dicho contrato con Grupo Tech Bull no fueron llevados a cabo con dicha empresa, sino que fueron realizados con las empresas Proyectos y Diseños VME S.A. de C.V. para el año 2016 y Air Cap S.A. de C.V. para el año 2017.

Cabe señalar que en diversas jurisdicciones es necesaria una autorización o licencia para la comercialización de equipos o sistemas para tareas de intervención de comunicaciones privadas de manera similar a requisitos para la comercialización de armamento. Sin embargo, en México no existe regulación que exija requisito alguno para ofrecer productos y servicios de esta naturaleza, ni ningún otro tipo de control sobre las empresas que comercializan equipos y sistemas de vigilancia.

b. Sobreprecios en la adquisición de equipos y sistemas de vigilancia

Como consecuencia de las condiciones de discrecionalidad y opacidad, con frecuencia los montos y condiciones de contratación de equipos y sistemas de vigilancia son exorbitantes e irrazonables.

Por ejemplo, en el contrato entre la Dirección General de Cuerpo Técnico de Control de la Subprocuraduría Especializada en Investigación de Delincuencia Organizada (SEIDO) y la empresa Neolinx de México S.A. de C.V. para "*la Prestación del Servicio de Localización Geográfica en Tiempo Real, para Equipos de Comunicación Móvil Asociados a una Línea Telefónica*", se adquirió la capacidad de 255 mil 500 búsquedas de monitoreo de la localización geográfica de equipos de comunicación móvil dentro de un plazo de 9 meses (de abril a diciembre de 2018).[4]

Cabe señalar que según datos reportados por la PGR a la Plataforma Nacional de Transparencia (PNT), durante el año 2018, dicha dependencia únicamente realizó 207 solicitudes de localización geográfica en tiempo real. Igualmente, según datos del Poder Judicial de la Federación (PJF)[5], en 2018, recibió un total de 27,849 solicitudes de autorización judicial para intervención de comunicaciones privadas, geolocalización en tiempo real y acceso a datos conservados por concesionarias de telecomunicaciones por parte de todas las autoridades facultadas por la ley –no únicamente la PGR–.

---

[4] SEIDO. Anexo Técnico de la Contratación para la prestación del servicio de localización geográfica en tiempo real, para equipos de comunicación móvil asociados a una línea telefónica. Disponible en: https://r3d.mx/wp-content/uploads/Anexo-tecnico-Geomatrix-SEIDO.pdf

[5] Presidente de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal. Informe Anual de Labores. Disponible en: https://www.cjf.gob.mx/resources/InformeAnual/2018/Informe_Anual_Labores_2018.pdf

De lo anterior se desprende un amplio diferencial que solamente puede ser explicado de dos maneras. La utilización masivamente ilegal del sistema de localización geográfica contratado o la enorme subutilización del sistema y consecuente despilfarro de recursos públicos.

Es el mismo caso del sistema *Pegasus*, el cual fue contratado en 2014, con dos renovaciones para los años 2016 y 2017 por montos que oscilan los 40 millones de dólares totales, sin embargo, como la PGR afirmó en el proceso de verificación identificado con la clave INAI.3S.07.01-007/2018, dicha dependencia "no lo utilizó"[6]. De nuevo se contempla la posibilidad de una subutilización y el consecuente dispendio injustificado de recursos públicos o, en su caso, la utilización ilegal no reportada del sistema, aunada a la falsedad de declaraciones ante el INAI. Al respecto, la Unidad de Inteligencia Financiera (UIF) de la Secretaría de Hacienda y Crédito Público ha afirmado públicamente haber detectado la adquisición de licencias de *Pegasus* con sobreprecio[7].

c. Ocultamiento y ofuscación de contrataciones

Con frecuencia, las contrataciones de equipos y sistemas de vigilancia pretenden ser escondidas u ofuscadas a partir de descripciones vagas del objeto de las contrataciones.

Por ejemplo, en el contrato realizado por la Procuraduría General de la República (PGR) para la adquisición de licencias del *spyware Pegasus*, dicho sistema fue denominado "*sistema para la realización de actividades sustantivas*", mientras que la SEDENA lo ha denominado "Sistema de Monitoreo Remoto de Información".

De igual manera, en contratos para la adquisición de antenas falsas para la intervención de comunicaciones se han utilizado denominaciones como "*adquisición de equipo activo GSM, para identificación y monitoreo*" o "*fortalecimiento de capacidades para la prevención y combate a delitos de alto impacto*". De manera similar, contratos relacionados a sistemas de análisis forense de dispositivos, como "*Cellebrite*", han sido objeto de contratos denominados "*mobiliario y equipo especializado para chequeo diagnóstico y demás*".

Asimismo, la gran mayoría de contratos relacionados con tareas de vigilancia detectados vía solicitudes de acceso a la información pública o investigaciones periodísticas, no aparecen en Compranet, lo que hace aún más difícil identificarlos[8] y detectar irregularidades en los mismos.

---

[6] Versión estenográfica de la sesión ordinaria del Pleno del INAI del día 20 de Febrero de 2019 en donde se resolvió el proceso de verificación identificado con la clave INAI.3S.07.01-007/2018. Páginas 25-26, 35-36.

[7] Zerega, Georgina, "El Gobierno de López Obrador asegura que hubo fraude en la compra del 'software' espía Pegasus", *El País*, 16 de febrero de 2024, disponible en: https://elpais.com/mexico/2024-02-16/el-gobierno-de-lopez-obrador-asegura-que-hubo-fraude-en-la-compra-del-software-espia-pegasus.html

[8] Ver por ejemplo: SSP/PF/CNS/026/2012 - Secretaría de Seguridad Pública - NUNVAV INC - 08/06/2012. Prestación del Servicio de Mantenimiento del Sistema Laguna para la Operación, Análisis y Monitoreo de localización de sistemas de telecomunicaciones y radiocomunicaciones, que operan en el espectro radioeléctrico mexicano.

De igual manera, aquéllas que sí aparecen en Compranet frecuentemente no contienen anexos, lo cual impide el acceso efectivo a detalles de dichas contrataciones.[9]

De esta manera, se dificulta la identificación de procesos de contratación relacionados a la adquisición de herramientas y sistemas utilizados en la vigilancia de comunicaciones, lo cual evita la detección de irregularidades en dichos procesos de contratación por parte de organizaciones periodísticas y de defensa de derechos humanos, e incluso, dificulta el ejercicio de facultades de investigación, por ejemplo, en procesos de verificación llevados a cabo por el INAI o en las carpetas de investigación abiertas por las fiscalías.

Aunado a lo anterior, se ha documentado como autoridades mienten con frecuencia para ocultar contrataciones relacionadas a la vigilancia de comunicaciones. Un caso emblemático es el de la SEDENA, respecto del cual se ha documentado que ha mentido en múltiples respuestas a solicitudes de acceso a la información, en las que ha afirmado falsamente no haber celebrado contrataciones con Comercializadora Antsua S.A. de C.V. —designada por NSO Group como distribuidora exclusiva de *Pegasus*— a pesar de que en documentos enviados a la Auditoría Superior de la Federación y otros documentos internos filtrados se reconoce y evidencia dicha contratación.

d. Ausencia de controles para evitar la adquisición ilegal de tecnologías de vigilancia

A partir de que en México los procesos de adquisición de equipos y sistemas para la vigilancia de comunicaciones no requieren un procedimiento o autorización especial y suelen únicamente involucrar a la autoridad y empresas contratantes, sin la intervención de ninguna otra dependencia, se ha fomentado la realización de contrataciones por parte de autoridades sin facultades de vigilancia de comunicaciones.

Por ejemplo, se ha reportado la adquisición del malware *Pegasus* por parte de la SEDENA y su utilización por parte del Centro Militar de Inteligencia, a pesar de que la SEDENA no cuenta con facultades para operar dicha herramienta para tareas de inteligencia. De igual manera, se ha documentado la adquisición de licencias para el uso de malware de vigilancia comercializado por la empresa italiana *Hacking Team* por parte de múltiples autoridades sin facultades. Por ejemplo, la Secretaría de Gobierno del Estado de Jalisco, la Secretaría de Planeación y Finanzas del Gobierno de Baja California o incluso Petróleos Mexicanos[10].

Adicionalmente, a pesar de que la Constitución, los tratados internacionales de derechos humanos y las leyes imponen límites a las autoridades respecto de las injerencias en la vida privada que resultan admisibles, no existe ningún mecanismo capaz de detectar y evitar que

---

[9] Ver por ejemplo: Expediente 355213 - REQ. 5415 SERVICIO DE INFORMATICA - SEMAR; Expediente 355202 - REQ. 5414 SERVICIOS DE INFORMATICA - SEMAR; Expediente 580008 - REQ. 0402 BIENES INFORMATICOS - SEMAR; y Expediente 1851475 - ADQUISICIÓN DE REFACCIONES PARA EQUIPOS DE RADIOCOMUNICACIÓN TÁCTICA EN HF - SEDENA.

[10] R3D. El Estado de la Vigilancia. Noviembre de 2016. Página 83. Disponible en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

sean adquiridos equipos y sistemas que excedan esos límites o faciliten la elusión de mecanismos de rendición de cuentas.

Por ejemplo, a pesar de que la intervención de comunicaciones privadas únicamente es admisible cuando exista una autorización judicial federal que justifique la utilización de dicha medida de manera focalizada, se ha documentado la adquisición de herramientas y sistemas que permiten injerencias en la vida privada y las comunicaciones privadas de manera masiva; es decir, respecto de un número amplio o indeterminado de personas. Es el caso de las antenas falsas, también conocidas como "IMSI catchers", las cuáles en su operación interfieren con un número indeterminado de personas que se encuentran en la proximidad de dichas antenas, por lo que la legalidad de su operación es altamente cuestionable, y en el mismo sentido, su adquisición.

Igualmente, resulta problemática la adquisición de sistemas diseñados para eludir la rendición de cuentas, es decir, sistemas que no dejan rastros o registros de su operación, dificultando procesos de investigación futuros sobre denuncias de abuso de dichos sistemas, como es el caso del malware *Pegasus*.

Cabe señalar que existen experiencias de regulación que exigen la obtención de autorizaciones y el registro de adquisiciones o exportaciones respecto de bienes como armas, municiones, vehículos o "tecnologías de doble uso", dentro de las cuales en ocasiones se ubican equipos y sistemas de vigilancia. Por ejemplo, en el artículo 124 de la Ley General del Sistema Nacional de Seguridad Pública se contempla el "Registro Nacional de Armamento y Equipo" en el que se incluyen vehículos y armamento. De manera similar, el Reglamento Europeo "por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso"[11] establece diversos procesos de autorización y registro respecto de bienes dentro de los cuales se ubican algunas tecnologías para la intervención de comunicaciones privadas.

De igual forma, es importante resaltar que las contrataciones públicas son un instrumento importante para la promoción de derechos humanos en México y en el mundo. De manera similar a otras legislaciones en el mundo,[12] México tiene la responsabilidad de asegurar que a través de las contrataciones públicas no está beneficiando a empresas involucradas en la violación de derechos humanos en cualquier parte del mundo.

Finalmente, la adquisición de este tipo de tecnologías desarrolladas en el extranjero puede conllevar riesgos en materia de seguridad nacional, respecto de los cuales no existe un proceso capaz de evaluar o remediar de manera previa o posterior a la adquisición y despliegue.

---

[11] Reglamento (CE) no 428/2009 del Consejo de 5 de mayo de 2009 por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso.

[12] Ver, por ejemplo la Sección 1502 de la "Dodd-Frank Wall Street Reform and Consumer Protection Act' de los Estados Unidos sobre la utilización de minerales en conflicto o el artículo 8 del Reglamento (CE) no 428/2009 del Consejo de 5 de mayo de 2009 por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso.

C. Ausencia de documentación sobre la adquisición y uso de equipos y sistemas de vigilancia

Aún cuando, como se ha afirmado, la legislación es deficiente en establecer procedimientos especializados para la adquisición y uso de equipos y sistemas de vigilancia, las autoridades suelen incumplir hasta los más mínimos requisitos de documentación.

Con frecuencia, las autoridades han afirmado no contar con información básica de los procesos de contratación, como estudios de mercado, opiniones de las áreas correspondientes o registros de cadena de custodia de los equipos. Al grado que en algunas ocasiones no ha sido posible verificar la ubicación material de los equipos y sistemas.

Adicionalmente, a pesar de que el marco jurídico exige la existencia de registros sobre las medidas de vigilancia de comunicaciones, con frecuencia las autoridades alegan la inexistencia de dichos registros.

Esta ausencia de documentación fomenta el abuso, obstaculiza la transparencia y el ejercicio de las facultades de supervisión e investigación que poseen diversas autoridades, lo cual también favorece la impunidad.

D. Vigilancia ilegal

Además de la adquisición y uso de equipos y sistemas de vigilancia de comunicaciones por parte de autoridades sin facultades legales para ello, existe amplia evidencia del abuso de dichas herramientas.

a. Espionaje a personas periodistas, defensoras de derechos humanos, activistas y opositoras políticas

Como se establece con detalle en el Capítulo Tres del informe citado, existe abundante evidencia del reiterado uso ilegal de herramientas de vigilancia de comunicaciones en contra de personas periodistas, defensoras de derechos humanos, activistas y opositoras políticas.

Por ejemplo, el uso de *spyware* como *Galileo* de la empresa italiana *Hacking Team*, respecto del cual existe evidencia que fue utilizado en contra de periodistas y políticos en estados como Puebla o Baja California, en donde inclusive personas admitieron culpabilidad ante el sistema judicial de Estados Unidos por comercializar y utilizar *spyware* ilegalmente y a sabiendas de su uso ilegal.

Se destaca la amplia evidencia de abuso del *spyware Pegasus*. Desde su adquisición y operación ilegal por parte de las áreas de inteligencia del ejército mexicano, así como su utilización en contra de periodistas, personas defensoras de derechos humanos y activistas.

También se destaca la evidencia de acceso ilegal a datos conservados por empresas de telecomunicaciones, así como el uso de tecnologías de vigilancia masiva respecto de periodistas, personas defensoras de derechos humanos, peritas independientes, funcionarios judiciales y opositores políticos.

La vigilancia de comunicaciones implica una grave interferencia en la vida privada de la persona vigilada, la cual ineludiblemente conlleva afectaciones a las personas con las que esa persona se comunica, incluyendo sus familiares cercanos y sus relaciones profesionales. Lo anterior posee una dimensión de gravedad aún mayor respecto de ciertas funciones profesionales.

Por ejemplo, la vigilancia a periodistas compromete a sus fuentes, poniendo en riesgo la revelación de su identidad e incluso su seguridad física. La vigilancia de personas defensoras de derechos humanos compromete la secrecía de las comunicaciones de personas abogadas con defensores y compromete información de víctimas de violaciones a derechos humanos. Asimismo, la vigilancia de personas que ejercen una función pública puede comprometer el ejercicio de sus funciones, haciéndoles vulnerables a la extorsión y el chantaje y, con ello, modificar sus decisiones en perjuicio del interés público y en beneficio de la persona o entidad que ejerce o se beneficia de la vigilancia.

Así, al afectar actividades como el periodismo, la defensa de derechos humanos o la integridad de las instituciones democráticas, la vigilancia ilegal con frecuencia conlleva una afectación a la sociedad y a sus aspiraciones democráticas, permitiendo a quien vigila con impunidad ejercer un control e influencia indebida en la sociedad y sus instituciones.

Adicionalmente, es crucial apreciar que la vigilancia ilegal con frecuencia se encuentra aparejada a otras formas de intimidación. Desde ataques reputacionales, extorsión, allanamientos, infiltración u operaciones psicológicas hasta potenciar o facilitar agresiones físicas, incluyendo el asesinato, como es el caso de los periodistas Fredid Román Román y Cecilio Pineda Brito, respecto de los cuales —como se documenta en el Informe citado— existen indicios de haber sido vigilados en momentos previos a su asesinato.

b. Acceso ilegal a datos conservados por empresas de telecomunicaciones

Como ha sido documentado, existen graves irregularidades en el sistema de acceso a datos de las comunicaciones de las personas usuarias de telecomunicaciones conservadas por las empresas que prestan dichos servicios.

Por un lado, existen serias discrepancias entre el número de accesos reportados por las autoridades facultadas, el Poder Judicial Federal y las empresas de telecomunicaciones, sugiriendo una práctica generalizada de acceso ilegal a estos datos, como es el mencionado caso del acceso ilegal a los datos de la periodista Marcela Turati; la cofundadora del Equipo Argentino de Antropología Forense (EAAF), Mercedes Doretti, y la defensora de derechos humanos Ana Lorena Delgadillo.

Adicionalmente, se reitera la evidencia de que el mecanismo excepcional contemplado en el artículo 303 del CNPP, por el cual autoridades pueden solicitar directamente el acceso a los datos sin control judicial previo, ha sido sistemáticamente abusado para obtener dicha información sin control judicial alguno.

Como es detallado en el Informe citado, se ha apreciado un *modus operandi* en el que las fiscalías utilizan carpetas sobre secuestro u otros delitos graves con la intención de eludir la obligación de obtener autorización judicial federal de manera previa. Además, en ningún caso someten a ratificación judicial las solicitudes de acceso a datos conservados, contraviniendo lo establecido en el artículo 303 del CNPP. Para ello, argumentan que, al no encontrar utilidad en la información, no resultaba necesario solicitar la ratificación judicial, por lo que (supuestamente) se procedió a su destrucción, sin que ello pueda ser verificado.

c. Geolocalización ilegal

Además de que las irregularidades detectadas en los esquemas de acceso a datos conservados por empresas de telecomunicaciones son aplicables a la geolocalización en tiempo real, existe evidencia de geolocalizaciones ilegales llevadas a cabo de manera autónoma por múltiples autoridades en México.

Destaca la proliferación de sistemas de geolocalización que explotan vulnerabilidades en el protocolo SS7 como *Geomatrix* de la empresa *Rayzone Group* y otras herramientas similares, las cuales han sido adquiridas por más de veinte autoridades, muchas de ellas sin facultades legales para llevar a cabo la geolocalización y utilizadas de manera discrecional y clandestina, sin ningún tipo de control judicial previo o inmediato. También sobresale el caso de la Fiscalía General de la República, respecto del cual la Auditoría Superior de la Federación documentó la adquisición y uso irregular del sistema *Geomatrix*.

Con frecuencia se subestima la sensibilidad de los datos de localización. Sin embargo, como ya ha sido explicado, los datos de localización permiten derivar el conocimiento de hábitos de movimiento de los que pueden desprenderse aspectos íntimos de la vida de una persona.

La vigilancia de una persona por medio de la geolocalización de su dispositivo móvil también permite identificar fuentes periodísticas, relaciones personales y patrones de movimiento capaces de frustrar actividades de interés público, realizar ataques reputacionales, facilitar la extorsión, e incluso, potenciar amenazas a la seguridad física y la vida de las personas. Ejemplo de lo anterior, resulta el mencionado asesinato del periodista Fredid Román Román cuyo teléfono fue geolocalizado un día antes de su asesinato en Chilpancingo, Guerrero, el 22 de agosto de 2022.

d. Empleo de tecnologías de vigilancia masiva

A partir de los principios de necesidad y proporcionalidad, las medidas de vigilancia únicamente pueden ser consideradas legítimas, si constituyen la alternativa menos lesiva disponible para conseguir un objetivo legítimo y si, después de un ejercicio de ponderación, las afectaciones a la privacidad y la seguridad no resultan exageradas o desmedidas frente a las ventajas obtenidas la vigilancia propuesta.

Lo anterior implica que, por constituir una afectación indiscriminada de los derechos de una cantidad indeterminada de personas, la vigilancia masiva no puede, en ningún caso, considerarse una medida legítima por parte del Estado, sino que la vigilancia debe ser focalizada y justificada por las circunstancias específicas de un caso concreto.

Sin embargo, se ha documentado la adquisición y operación ilegal de herramientas de vigilancia masiva, como lo son las antenas falsas (también conocidas como *IMSI catchers* o *stingrays*) por parte de múltiples autoridades en México. La operación de estos sistemas se realiza sin ningún tipo de control judicial o administrativo. Además existe evidencia de su despliegue en zonas del centro histórico de la Ciudad de México en donde suelen ocurrir protestas, lo cual potencialmente implica la vigilancia e identificación de las personas asistentes.

Adicionalmente, recientemente se ha detectado el uso de otras formas de vigilancia masiva como la herramienta *Echo*, desarrollada por Rayzone Group, la cual permite a autoridades realizar búsquedas de información sobre personas en un sistema que recolecta masivamente información sobre personas usuarias de servicios y aplicaciones en Internet.

Este *outsourcing* de la vigilancia masiva constituye una novedosa manera de intentar eludir las limitaciones constitucionales a la vigilancia que el poder público puede ejercer sobre la población. Sin embargo, así como no resulta legítimo que el Estado construya y opere un sistema de vigilancia masiva sobre las población, mediante la recolección y sistematización de datos obtenidos de su navegación en sitios y aplicaciones en Internet, tampoco resulta compatible con las normas de derechos humanos delegar esa vigilancia masiva a particulares.

E. Control judicial inefectivo

Como ha sido explicado, el marco jurídico mexicano es claro en establecer un control judicial federal sobre las medidas de vigilancia de comunicaciones. Sin embargo, también ha sido documentado como este control judicial es frecuentemente eludido.

Las enormes discrepancias entre los datos estadísticos reportados por autoridades que llevan a cabo medidas de vigilancia, el poder judicial federal y empresas de telecomunicaciones son indicativos de una práctica generalizada de elusión del control judicial federal.

También, la evidencia demuestra que el mecanismo excepcional contemplado en el artículo 303 del CNPP, para solicitar directamente el acceso a datos conservados a las empresas de telecomunicaciones sin control judicial previo y sujeto a la ratificación posterior por parte de la

autoridad judicial federal, se ha convertido en la regla general y es frecuentemente abusado para eludir el control judicial efectivo.

Como la información estadística documentada en el Informe citado indica, la mayoría de las solicitudes de acceso a datos conservados no han contado con control judicial federal previo. Además, de aquéllas en las que se han invocado las causales de excepción a las que se refiere el artículo 303 del CNPP, cerca del 40% no son ratificadas por la autoridad judicial federal, denotando su improcedencia original.

Aunado a ello, existen indicios adicionales de que un numero significativo de medidas de vigilancia en las que la autoridad alega causales de excepción al control judicial previo, ni siquiera son sometidas al proceso de ratificación judicial. Este *modus operandi*, como ha sido reportado, ha sido utilizado para la vigilancia ilegal.

Por si no fuera suficiente, el control judicial federal se ha hecho aún más improbable respecto de las medidas de vigilancia de comunicaciones desplegadas de manera autónoma por las autoridades, es decir, sin requerir la colaboración de empresas de telecomunicaciones y otros entes.

La utilización *spyware* en contra de decenas de periodistas, personas defensoras de derechos humanos, funcionarios públicos y otras, se ha llevado a cabo sin ningún tipo de control judicial. Lo mismo ha sucedido con herramientas como las antenas falsas, la geolocalización mediante sistemas como *Geomatrix* o *Echo*, e incluso en la operación de herramientas de extracción forense como *Cellebrite*.

La evidencia demuestra la facilidad con la que las autoridades pueden eludir el control judicial, las pocas posibilidades de que esa elusión sea detectada y las aún menores probabilidades de que ante la documentación de la vigilancia sin control judicial exista algún tipo de consecuencia.

Aún en los casos en los que existe autorización judicial federal, no existe evidencia de que el Poder Judicial Federal ejerza efectivamente sus facultades de supervisión para evaluar si la implementación de las medidas de vigilancia se adecúan a los términos autorizados.

En resumen, las disposiciones normativas que disponen el control judicial federal previo o inmediato de las medidas de vigilancia, por sí solas no han garantizado un control judicial efectivo y requieren estar complementadas de otros sistemas de control para garantizar su efectividad práctica.

Sin control judicial efectivo, las autoridades con capacidades para llevar a cabo medidas de vigilancia cuentan con amplias garantías de que su utilización ilegal será difícilmente detectada y sancionada, fomentando así la continuación y repetición de los abusos.

F. Ausencia de documentación y registro de actividades de vigilancia

La prevención, detección e impunidad de abusos en el despliegue de actividades de vigilancia de comunicaciones se encuentra importantemente obstaculizada por la ausencia de documentación y el ocultamiento deliberado de la misma.

La ausencia de documentación clave sobre los procesos de adquisición de equipos y sistemas de vigilancia y sobre las empresas que comercializan dichos productos y servicios, fomentan la corrupción, la adquisición y operación ilegal de los mismos y la dificultad de investigar a los responsables.

A pesar de que el marco jurídico establece la obligación de establecer registros de las intervenciones de comunicaciones privadas, las autoridades frecuentemente niegan la existencia de los mismos. La ausencia o inaccesibilidad de los registros constituyen serios obstáculos para la supervisión de las medidas de vigilancia y la investigación de probables abusos. Esto se exacerba frente a la creciente proliferación de equipos y sistemas de vigilancia como el *spyware*, que además de ser operadas de manera autónoma, sin necesidad de colaboración de ente alguno y de poseer capacidades intrusivas amplias, contiene medidas para dificultar su detección.

Si bien fabricantes de este tipo de este tipo de tecnologías como *NSO Group* han afirmado que tecnologías de *spyware* como *Pegasus* poseen funcionalidades de registro (*logging)* que permiten la auditoría del sistema para identificar los objetivos del mismo, autoridades han negado la existencia de dicho registro y el mismo no puede ser accedido sin colaboración del ente investigado, por lo que ni la autoridad judicial, ni autoridades con facultades de investigación han sido capaces de acceder a dichos registros.

Sin requisitos estrictos de registro de los equipos y sistemas utilizados para desplegar facultades de vigilancia, de las empresas que los desarrollan y comercializan, de las autoridades que los adquieren y utilizan, así como registros de uso y despliegue de medidas de vigilancia de comunicaciones, dichas medidas permanecerán siendo inverificables, con la consecuencia de perpetuar los abusos y la impunidad.

G. Falta de transparencia

La transparencia permite el control social de la función pública, permite prevenir y detectar abusos y otorga a las autoridades con facultades para investigarlos herramientas claves para evitar la impunidad de los mismos. Crucialmente la transparencia también permite contar con evidencia para evaluar los riesgos y beneficios de determinadas políticas públicas. La transparencia respecto de medidas de vigilancia no es la excepción.

Aún cuando la vigilancia de comunicaciones se encuentra frecuentemente relacionada a actividades respecto de las cuales cierta secrecía resulta necesaria para su efectividad, como la seguridad pública, la investigación de delitos o la atención de amenazas a la seguridad nacional, ciertas medidas de transparencia respecto de estas actividades resultan cruciales

para prevenir y detectar abusos, así como para evaluar, con base en evidencia, si los objetivos de interés público que frecuentemente son aludidos para justificar la vigilancia de comunicaciones son conseguidos o si en el despliegue de este tipo de medidas existen actos de corrupción o inadecuados controles frente a potenciales abusos.

Como ha sido expuesto, el marco jurídico mexicano —especialmente el artículo 70, fracción XLVII, de la LGTAIP— dispone medidas de transparencia estadística respecto de las medidas de vigilancia. De igual manera, órganos garantes en materia de transparencia y el Poder Judicial de la Federación han realizado interpretaciones que han permitido reconocer la publicidad de diversa información vinculada a medidas de vigilancia y de los abusos relacionados a la misma. Sin embargo, persisten serios obstáculos para la efectividad de las medidas de transparencia.

a. El incumplimiento de las obligaciones de transparencia oficiosa establecidas en el artículo 70, fracción XLVII de la LGTAIP por parte de las autoridades que llevan a cabo medidas de vigilancia.

Como se ha documentado previamente[13], existen graves incumplimientos a las obligaciones de transparencia oficiosa que establece el artículo 70, fracción XLVII de la LGTAIP.

De 2020 a 2023, únicamente dos autoridades federales (FGR y Guardia Nacional) y seis fiscalías estatales han publicado información estadística completa en la PNT respecto de medidas de intervención de comunicaciones privadas. Cuatro fiscalías estatales han publicado información incompleta. Otras autoridades federales como el Centro Nacional de Inteligencia y veintidós fiscalías estatales no han reportado información alguna a la PNT.

En el caso de información estadística sobre el acceso a datos conservados y geolocalización en tiempo real, únicamente dos autoridades federales y seis fiscalías estatales publicaron información estadística completa entre 2020 y 2023, mientras que otras once fiscalías estatales publicaron información incompleta en algunos trimestres. Otras autoridades federales y quince fiscalías estatales no reportaron información alguna a la PNT.

b. Información estadística incompleta y sin suficiente desagregación reportada a la PNT

Aún cuando las autoridades sí reportan información estadística a la PNT, existen varias circunstancias que reducen su utilidad y comparabilidad.

Por un lado, a pesar de que el marco jurídico mexicano establece la obligación de conservar registros fehacientes de las solicitudes de intervención de comunicaciones y de las decisiones judiciales relacionadas, y que el artículo 70, fracciones XXX y XLVII, de la LGTAIP obligan a producir información estadística “con la mayor desagregación posible”, la información que es

[13] R3D, *Transparencia y Vigilancia,* 2019. Disponible en: https://r3d.mx/wp-content/uploads/TRANSPARENCIA-Y-VIGILANCIA-2019.pdf

efectivamente reportada a la PNT o entregada en respuesta a solicitudes de acceso a la información no cumple con dichos parámetros.

Frecuentemente algunas autoridades alegan no contar con la información estadística sobre medidas de vigilancia con el nivel de desagregación que se solicita. Es decir, diversas autoridades no conservan un registro "fehaciente" ni "con la mayor desagregación posible" de las solicitudes y resoluciones de autorización judicial en torno a medidas de vigilancia.

Los "Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia"[14] publicados por el INAI, limitan de manera trascendental la efectividad de las obligaciones de transparencia oficiosa al limitar la obligación de reporte a que se refiere la fracción XLVII del artículo 70 de la LGTAIP al únicamente requerir que sea enlistada la información sobre medidas de vigilancia cuando las mismas se encuentren "concluidas, es decir, que no formen parte de una investigación en curso".

Lo anterior reduce drásticamente la utilidad de las estadísticas reportadas, pues no permite conocer el volumen real de solicitudes. Lo anterior se agrava dado el hecho de que, por ejemplo, según el Censo Nacional de Procuración de Justicia Estatal 2021 publicado por el INEGI, la inmensa mayoría de las carpetas de investigación no se encuentran concluidas[15]. Además resulta contradictorio con decisiones previas del INAI y de la SCJN en torno a que el reporte de esta información estadística de ninguna manera puede considerarse que pone en riesgo ninguna investigación ni ningún interés público, como la procuración de justicia, la seguridad pública o la seguridad nacional.

De igual manera, los mencionados lineamientos agregan en el mismo campo estadístico la solicitudes de acceso a datos conservados y las de localización geográfica en tiempo real, lo cual de nuevo contraviene la obligación de "mayor desagregación posible" y reducen la utilidad y comparabilidad de la información estadística.

c. Ausencia e incomparabilidad de información estadística por parte del Poder Judicial de la Federación.

A pesar de que el artículo 70, fracción XLVII de la LGTAIP no excluye al Poder Judicial de la Federación (PJF) en el cumplimiento de la obligación de transparencia oficiosa en relación a estadísticas relacionadas a las solicitudes sobre medidas de vigilancia, el INAI recientemente dispuso excluir de su cumplimiento al PJF.

---

[14] Disponibles en: https://snt.org.mx/wp-content/uploads/Lineamientos-Tecnicos-Generales-Version-Integrada.pdf

[15] INEGI, Censo Nacional de Procuración de Justicia Estatal 2021. 19 de mayo de 2023. Disponibles en: https://www.inegi.org.mx/contenidos/programas/cnpje/2021/doc/cnpje_2021_resultados.pdf

En efecto, el INAI eximió al Consejo de la Judicatura Federal (CJF) de la obligación de transparencia oficiosa contenida en el artículo 70, fracción XLVII de la LGTAIP a partir de la "Modificación a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Consejo de la Judicatura Federal, emitida por el INAI y publicada en el Diario Oficial de la Federación el 12 de julio de 2018".

Lo anterior implica que no existe manera de contrastar la información aportada por las autoridades con facultades de vigilancia a la Plataforma Nacional de Transparencia (PNT) con la información que el PJF debería publicar en dicha plataforma. Lo anterior resulta ser sumamente relevante en virtud de las inconsistencias entre las cifras reportadas por diversas autoridades que se desarrollan en el informe citado.

Si bien el CJF publica anualmente un informe estadístico sobre el número de asuntos que el Poder Judicial de la Federación conoce respecto de solicitudes de autorización judicial federal de medidas de vigilancia como la intervención de comunicaciones privadas y el acceso a datos conservados por empresas de telecomunicaciones, dicha información carece de la especificidad y granularidad para hacerla comparable con otras fuentes de información. Destacadamente, dicha información no desagrega los datos por autoridad solicitante, ni en los periodos de tiempo que permitirían contrastar con la información reportada por las propias autoridades solicitantes, lo cual de nuevo implica una violación al principio de "máxima desagregación posible".

d. La reserva absoluta de solicitudes y resoluciones relacionadas a la autorización de medidas de vigilancia, ante la ausencia de medidas de transparencia estadística suficientes y a las inconsistencias en el reporte de las mismas.

Dado que existe amplia evidencia de inconsistencias entre la información estadística reportada por autoridades en la PNT, la información entregada a partir de solicitudes de acceso a la información y la información publicada, en su momento, por el IFT, así como ante la ausencia del cumplimiento de obligaciones de transparencia oficiosa con el máximo nivel de desagregación posible, se hace indispensable permitir a la sociedad acceder a las versiones públicas de las solicitudes y autorizaciones judiciales relacionadas a medidas de vigilancia, de manera que pueda contrastarse adicionalmente la información estadística reportada en el PNT o ante solicitudes de acceso a la información con la información que se desprende directamente de los documentos que son fuente de ese cálculo estadístico.

No obstante lo anterior, persisten autoridades, e incluso órganos garantes, que pretenden establecer reservas absolutas en el acceso a los documentos de los que se puede desprender la veracidad o falsedad de las estadísticas reportadas.

Por ejemplo, el CJF, además de haber sido excluido arbitrariamente por el INAI del cumplimiento de las obligaciones de transparencia oficiosa a las que se refiere el artículo 70,

fracción XLVII de la LGTAIP, y de no reportar información estadística con el máximo nivel de desagregación posible, ha considerado la reserva absoluta de la información. Por lo que, el CJF no aporta la información estadística necesaria ni permite a la sociedad generarla de manera propia a partir del acceso a las versiones públicas de las solicitudes y resoluciones.

Además, con la reserva absoluta de las resoluciones de los jueces de control en torno a las solicitudes de autorización respecto de medidas de vigilancia, se impide a la sociedad conocer la manera en la que el PJF interpreta las normas relacionadas a las medidas de vigilancia, con lo cual se priva a la sociedad de conocer el contenido y alcance real de las medidas, lo cual resulta equivalente a no tener derecho a conocer las propias normas. Lo anterior contraviene además la obligación establecida en el artículo 73, fracción II de la LGTAIP la cual dispone la publicidad de "las versiones públicas de todas las sentencias emitidas" sin hacer distinción alguna.

Es importante resaltar que no se solicita acceso a los elementos fácticos de las solicitudes y resoluciones, como lo pueden ser nombres, números de teléfono u otros datos que identifiquen a las personas bajo investigación, ni los hechos que motivan la misma, sino que únicamente se solicita acceso a versiones públicas, que testen la información sensible pero permitan conocer y calcular, información estadística anonimizada y la manera en la que la autoridad judicial interpreta y define el contenido y alcance de las normas que regulan las medidas de vigilancia.

Por lo tanto, no es razonable la noción de que el acceso a versiones públicas de dichos documentos ponga en riesgo investigación alguna o los intereses de la procuración de justicia, seguridad pública o seguridad nacional.

e. La ausencia de obligaciones de transparencia para empresas que colaboran en materia de vigilancia

Al emitir los Lineamientos de Colaboración en Materia de Seguridad y Justicia publicados en el Diario Oficial de la Federación el 2 de diciembre de 2015[16], el Instituto Federal de Telecomunicaciones contempló disposiciones encaminadas a favorecer la transparencia en la colaboración en materia de seguridad y justicia. En concreto, el Lineamiento Décimo Octavo de dichos Lineamientos estableció la obligación de las concesionarias y autorizadas de telecomunicaciones de entregar al IFT un informe semestral que debía contener información estadística como el número de requerimientos recibidos y cumplimentados de parte de autoridades facultadas, los cuáles serían publicados por el Instituto en su portal de Internet.

La producción y publicación de estos informes durante los años 2016 y 2017 permitió al Instituto y al público en general, conocer información relevante sobre las medidas de colaboración en materia de seguridad y justicia.

---

[16] Lineamientos de Colaboración en Materia de Seguridad y Justicia. 2 de diciembre de 2015. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

Por ejemplo, destaca que, entre los años 2016 y 2017, los concesionarios y autorizados de telecomunicaciones reportaron haber recibido poco más de 140 mil solicitudes de acceso a datos conservados y de geolocalización, de las cuales, en 97 por ciento de las ocasiones, la información fue entregada. Así mismo, 31.5 por ciento de las solicitudes reportadas –casi la tercera parte– fueron realizadas por autoridades sin facultades o cuya identidad no se conoce[17].

De manera preocupante, los datos reportados revelan que las empresas Telcel y Telmex entregaron información en el 100 por ciento de las solicitudes recibidas (110,214 y 6,402, respectivamente), en tanto que Movistar otorgó los datos en 83.4 por ciento de las ocasiones; y AT&T, en 61.5 por ciento. Es importante destacar que el 31 por ciento de las solicitudes recibidas por Telcel (y entregadas en su totalidad) fueron efectuadas por autoridades sin facultades o no identificadas[18].

No obstante la relevancia pública de la información contenida en los informes requeridos por el Instituto con base en los Lineamientos y de la utilidad para el ejercicio de las facultades propias del Instituto relacionadas con la protección del derecho a la privacidad, el Instituto decidió eliminar dichas obligaciones en abril de 2018[19], por lo que hoy no es posible para el Instituto y para los usuarios conocer el número de solicitudes de acceso a usuarios que recibe cada concesionario o autorizado, las autoridades solicitantes o el número de solicitudes que son cumplidas o negadas por los concesionarios o autorizados.

Esta decisión inexplicable del IFT ha privado a la sociedad de la posibilidad de contrastar la información reportada por las empresas de telecomunicaciones con la información reportada por autoridades y por el Poder Judicial de la Federación, aunado a que ha privado al IFT de información necesaria para ejercer sus facultades, como la establecida en el artículo 298, apartado D), fracción V de la LFTR, la cual otorga al Instituto la facultad imponer sanciones a los concesionarios o autorizados cuando no establezcan las medidas necesarias para garantizar la confidencialidad y privacidad de las comunicaciones de los usuarios.

Positivamente, en agosto de 2024, el IFT presentó un Anteproyecto de modificación a los Lineamientos en el que, entre otras cosas, reincorpora la obligación de producir informes estadísticos por parte de las empresas concesionarias en materia de telecomunicaciones. Sin embargo, al cierre de edición del presente informe la modificación no ha sido materializada.

Finalmente, también debe señalarse que aunque algunas empresas proveedoras de aplicaciones, contenidos y servicios en Internet voluntariamente publican informes de transparencia en los que ofrecen alguna información estadística sobre las solicitudes provenientes de autoridades para el acceso a datos de personas usuarias, dicha información

---

[17] R3D. Quién No Defiende Tus Datos. 2018. Disponible en: https://r3d.mx/wp-content/uploads/R3D-QNDTD_digital.pdf

[18] *Ídem.*

[19] Modificación a los Lineamientos de Colaboración en Materia de Seguridad y Justicia. Publicada en el Diario Oficial de la Federación el 2 de abril de 2018. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5517853&fecha=02/04/2018

carece de granularidad y especificidad relevante para poder ser contrastada con otras fuentes de información.

f. La reserva excesiva de información y versiones públicas de documentos sobre aspectos técnicos de las herramientas y equipos utilizados para llevar a cabo medidas de vigilancia

Frecuentemente, las respuestas a solicitudes de acceso a la información relacionadas a documentos que forman parte de procesos de contratación relacionados a equipos y sistemas de vigilancia frecuentemente son reservados de manera absoluta o excesiva.

Algunos precedentes del INAI[20] otros órganos garantes[21], e incluso en el Poder Judicial de la Federación[22] han reconocido, que la reserva absoluta o excesiva de contratos y anexos técnicos relacionados a equipos y sistemas sobre la intervención de comunicaciones privadas viola el derecho de acceso a la información.

De parte de las autoridades y del INAI ha persistido la posición de que algunas categorías de información deben permanecer reservadas, en específico, las especificaciones técnicas de los equipos y sistemas adquiridos y los datos que identifican a los funcionarios que participan en los procesos de adquisición.

Desde nuestra perspectiva, la reserva de esas categorías de información obstaculiza de manera innecesaria el derecho de acceso a la información. Por ejemplo, respecto de las especificaciones técnicas de equipos y sistemas adquiridos, el análisis de parte de las autoridades y del INAI ha sido sumamente superficial, en tanto se asume que la revelación de dicha información, en todos los casos, reduce la efectividad o permite eludir los sistemas o equipos de intervención de comunicaciones cuando no se presenta ninguna evidencia de ello ni se realiza un análisis de dichas aseveraciones.

Por el contrario, las especificaciones técnicas de múltiples equipos y sistemas de intervención de comunicaciones privadas han sido publicados en el pasado sin que exista evidencia de que dichas publicaciones hayan reducido la efectividad de dichas herramientas.

Este es el caso relacionado con el *spyware* “Pegasus”, respecto del cual se conocen sus capacidad y características técnicas desde hace muchos años sin que dicho conocimiento haya frustrado de manera alguna su efectividad.

---

[20] *Véase* INAI. RRA 11072/19. Resolución del recurso de revisión interpuesto en contra de la respuesta del Centro Nacional de Inteligencia. 11 de diciembre de 2019.

[21] Comisión Estatal de Garantía de Acceso a la Información Pública del Estado de San Luis Potosí. RRA 588/2017-3. Resolución del recurso de revisión interpuesto en contra de la respuesta de la Oficialía Mayor. 20 de octubre de 2017.

[22] *Véase* Juzgado Octavo de Distrito en Materia Administrativa en la Ciudad de México. Juicio de Amparo 591/2018. Sentencia de 13 de diciembre de 2018. Disponible en: http://sise.cjf.gob.mx/SVP/word1.aspx?arch=729/07290000228987130013012.docx_1&sec=Jos%C3%A9_Sebasti%C3%A1n__G%C3%B3mez_S%C3%A1mano&svp=1

Es importante resaltar que el conocimiento de información técnica, en específico, las capacidades generales de los equipos y sistemas, es fundamental para que las personas podamos conocer las capacidades invasivas del Estado, así como evaluar y fiscalizar la pertinencia de la operación de dichas herramientas.

Igualmente, en múltiples solicitudes de acceso a la información, las autoridades únicamente reconocen la existencia de contratos y anexos técnicos, sin reconocer la existencia de documentación previa al contrato que, de conformidad con la legislación en la materia, debería existir dentro de un proceso de adquisición. En este sentido, se observa que tanto la ausencia de documentación de los procesos de adquisición y uso o, en su caso, la omisión en la entrega de las versiones públicas de dicha información afectan severamente la transparencia de dichos procesos de adquisición.

g. Avances en el reconocimiento de la publicidad de información indicios de abuso de las herramientas de vigilancia

Recientemente se han adoptado decisiones que han reconocido la publicidad de información relacionada a casos donde existen indicios y evidencia de abuso de equipos y sistemas para la vigilancia de comunicaciones.

Por ejemplo, el INAI ha emitido diversas resoluciones[23] en las que ha ordenado a la SEDENA entregar información sobre las contrataciones realizadas por dicha dependencia relacionadas con el *spyware Pegasus*. Igualmente, la SCJN reciente reconoció el interés público de información relacionada al Caso Pegasus en poder de la Unidad de Inteligencia Financiera[24]

Es importante que los órganos garantes en materia de transparencia, así como el Poder Judicial continúen reconociendo que, como establece el artículo 115 de la LGTAIP, las reservas de información no son procedentes cuando se trate de violaciones graves a derechos humanos o de información relacionada con actos de corrupción, conceptos que resultan aplicables a los casos en los que existen indicios o evidencia de un uso ilegal de medidas de vigilancia de comunicaciones.

h. Incumplimiento de resoluciones

A pesar de los precedentes recientes en los que se ha dispuesto la publicidad de información contractual y financiera relacionada a la adquisición de equipos y sistemas de vigilancia respecto de los cuales existe evidencia de adquisición irregular o uso ilegal, las mismas no han permitido conseguir una mayor transparencia respecto de esos procesos debido al incumplimiento de las resoluciones.

---

[23] *Véase*, por ejemplo: INAI, Sedena debe informar sobre contrataciones con Comercializadora Antsua S.A. de C.V. para monitoreo de información remota. Nota Informativa INAI/010/23, 29 de enero de 2023. Disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-010-23.pdf

[24] SCJN, Confirma la Corte resolución del INAI que ordena la entrega en versión pública de información relativa al Caso Pegasus, 6 de febrero de 2024. Disponible en: https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=7708

Por ejemplo, como se documenta en el informe citado, a pesar de que el INAI ha emitido una resolución inatacable para la autoridad, ordenándole entregar los contratos relacionados al *spyware Pegasus*, la SEDENA se ha negado a cumplir con dicha resolución, e incluso ha impugnado una sentencia de amparo en la que un juez de distrito ha confirmado la obligatoriedad de la decisión.

Este ilegal e impune desacato de resoluciones de los órganos garantes en materia de transparencia atenta contra el derecho de acceso a la información pública, al mismo tiempo que demuestra la necesidad de que se establezcan mecanismos que permitan sancionar efectivamente estas conductas arbitrarias.

H. Ausencia de mecanismos de supervisión efectivos

A diferencia de la regulación existente en el derecho comparado, en México no existe un mecanismo de supervisión independiente explícitamente establecido para ejercer un control externo respecto del ejercicio de medidas de vigilancia. En su caso, el INAI posee ciertas facultades, a través de los procedimientos de verificación, para ejercer ciertas medidas de control, sin embargo, como ya ha sido adelantado, dichos procesos poseen diversas limitaciones y obstáculos.

Uno de los obstáculos más importantes es el plazo de duración máxima en la sustanciación de los procedimientos de verificación establecido en el artículo 149 de la Ley General de Protección de Datos en Posesión de Sujetos Obligados, el cual es aprovechado por las autoridades mediante medidas dilatorias, para complicar la labor del INAI en la sustanciación de dichos procedimientos, como ocurrió en el proceso de verificación INAI.3S.07.01-007/2018, en el que la entonces PGR fue encontrada en violación de sus obligaciones en materia de protección de datos personales.

Igualmente, los presupuestos de procedencia, las negativas de información aludiendo restricciones en materia de seguridad nacional, así como al carecer de medidas sancionatorias directas o suficientes, los efectos de dichos procedimientos son sumamente limitados y por ello no han sido efectivos para ejercer un control efectivo sobre las medidas de vigilancia estatal.

Como la Relatora Especial de la ONU sobre la lucha contra el terrorismo ha señalado, las decisiones sobre permitir el uso de *spyware* o las autorizaciones de exportación de los mismos, deben ir acompañadas de sólidas estrategias de debida diligencia para minimizar la posibilidad de daños derivados de esta potente e invasiva tecnología, así como de robustas funciones de registro y auditoría para que el uso indebido pueda investigarse, probarse y remediarse de forma eficaz. Estas auditorías deberán incluir algún mecanismos que permitan vincular en última instancia el *spyware* con sus productores y clientes gubernamentales, para que se pueda acceder a remedios adecuados en contra del productor o gobierno que los utiliza.[25]

---

[25] Relatora Especial sobre la Lucha contra el Terrorismo, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, op. Cit. 28, pár. 59.

Sin embargo, el marco jurídico mexicano no dispone de mecanismos de supervisión independientes, capaces de llevar a cabo auditorías aleatorias sobre las medidas de vigilancia, lo cual de nuevo fomenta su abuso y la impunidad.

I. Impunidad

Como ha sido ampliamente documentado, en 2017, 2022 y 2023, las personas vigiladas por el *spyware Pegasus*, principalmente personas defensoras de derechos humanos y periodistas, presentaron denuncias penales ante la Fiscalía Especial para la Atención de Delitos Cometidos contra la Libertad de Expresión (FEADLE) por, entre otros, los delitos de intervención ilegal de comunicaciones privadas y acceso ilegal a sistemas informáticos. El hecho de que una de las víctimas, el Centro Prodh, haya sido objeto de vigilancia con *Pegasus* en dos administraciones distintas, y haya presentado dos denuncias penales diferentes, muestra cómo la impunidad y la falta de medidas adecuadas llevaron a la repetición de la vigilancia ilegal.

A pesar del llamado de múltiples instancias, nacionales e internacionales sobre la necesidad de llevar a cabo una investigación diligente, con garantías de autonomía reforzadas, más de siete años después del anuncio del inicio de la primera carpeta de investigación, y a más de dos años del inicio de la investigación sobre la repetición del espionaje ilegal, ninguna persona ha sido condenada por los hechos.

La Fiscalía, entre otras deficiencias, se ha negado a realizar actos esenciales de investigación, ha obstruido y fragmentado las investigaciones, ha hecho recaer la carga de la prueba en las víctimas y les ha negado copia de los expedientes.[26]

La justicia y la rendición de cuentas también son obstruidas por las autoridades denunciadas, quienes afirman sistemáticamente que no existe ninguna base de datos o documentación formal de los registros relativos a las personas o números atacados, a pesar de evidencia en contrario. En 2019, el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) determinó que la Fiscalía había incumplido sus obligaciones conforme a la legislación de Protección de Datos Personales al ocultar contratos con NSO Group.[27] Sin embargo, hasta la fecha, la Fiscalía General se ha negado a emprender cualquier investigación seria e independiente en relación con la obstrucción de la justicia documentada.

Decisions to allow spyware use or spyware export approvals are obliged to be accompanied with robust due diligence strategies to minimize the potential for gender harms arising from this powerful and invasive technology, and robust record-keeping and audit functions so that misuse can be efficiently investigated, evidenced, and remedied. These audit functions ought to include some mechanism of digital watermarking such that spyware can ultimately be linked to its producer and their governmental client, with the result that avenues of remedy (against producer or governmental user) can be accessed.

[26] Carpeta de investigación FEADLE FED/SDHPDSC/UNAI-CDMX/0000430/2017; Ahmed, Azam, “Mexico Spyware Inquiry Bogs Down. Skeptics Aren’t Surprised”, The New York Times, 20 de febrero de 2018, disponible en: https://www.nytimes.com/2018/02/20/world/americas/mexico-spyware-investigation.html; R3D: Red en Defensa de los Derechos Digitales, “A un año de #GobiernoEspía, prevalece la impunidad”, 20 de junio de 2018, disponible en: https://r3d.mx/2018/06/20/comunicado-a-un-ano-de-gobiernoespia-prevalece-la-impunidad/

[27] INAI, “Determina INAI que FGR, respecto al software Pegasus, incumplió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados”, 20 de febrero de 2019, disponible en: https://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf

Varias investigaciones aún no han dado señales de progreso. La única detención de una persona[28] —a quien se le imputó el delito de intervención telefónica por su probable participación como operador del software dentro de una de las empresas intermediarias entre la NSO Group y la PGR— sólo fue posible gracias a información proporcionada por una de las víctimas, que remitió a las autoridades a la red de intermediarios que comercializaba *Pegasus* en México.

A pesar de que se celebró un juicio en diciembre de 2023 contra dicho operador, en donde se confirmó mediante sentencia judicial la ilegal intervención de comunicaciones en contra de la periodista Carmen Aristegui, no han existido avances en la imputación de responsabilidades de funcionarios públicos de las dependencias como la PGR, el CISEN y el Ejército Mexicano, respecto de las cuáles existe amplia evidencia de haber adquirido y operado el spyware.

La renuencia de la Fiscalía a realizar diligencias en cuanto a líneas de investigación respecto de la Agencia de Investigación Criminal de la FGR demuestra la falta de autonomía, imparcialidad y profesionalismo en la investigación, máxime cuando tanto la autoridad que realiza la investigación, la FEADLE, como la única autoridad que ha admitido el uso del malware Pegasus, la AIC, forman parte de la misma Fiscalía General. Asimismo, no se han llevado a cabo acciones de investigación serias respecto al CISEN ni al Ejército Mexicano, con evidencias que los confirman como operadores de Pegasus durante el gobierno pasado.

Respecto a la más reciente investigación sobre el abuso de Pegasus por parte del Ejército entre 2019 y 2022, la Fiscalía no ha logrado ningún avance en más de dos años. Ni siquiera ha podido obtener los contratos en los que el Ejército obtuvo licencias para operar Pegasus. La SEDENA se ha negado a hacer públicos los contratos con NSO Group para la adquisición de Pegasus u otros sistemas de vigilancia, como prometió públicamente el Presidente.[29] Lo anterior a pesar de las numerosas pruebas y documentos que muestran el número y las fechas de los contratos, así como los pagos realizados por la SEDENA.

A pesar de la gravedad de las denuncias, México no ha aceptado el establecimiento de un mecanismo internacional de supervisión independiente y los documentos relacionados con la contratación y uso de Pegasus aún no han sido hechos públicos por las autoridades del Estado mexicano. El gobierno no sólo ha faltado a su obligación de garantizar la verdad y justicia a las víctimas, sino que ha perpetuado la impunidad y generado las condiciones para la repetición de los hechos.

---

[28] Article 19 MX-CA, “Avance del caso Pegasus en México debe ser un punto de no retorno que ayude a esclarecer un crimen de talla mundial”, 8 de noviembre de 2021, disponible en: https://articulo19.org/avance-del-caso-pegasus-en-mexico-debe-ser-un-punto-de-no-retorno-que-ayude-a-esclarecer-un-crimen-de-talla-mundial/%20; Aristegui Noticias, “Detiene FGR a uno de los involucrados en espionaje con Pegasus”, 8 de noviembre de 2021, disponible en: https://aristeguinoticias.com/0811/mexico/detiene-fgr-a-uno-de-los-involucrados-en-espionaje-con-pegasus/

[29] R3D: Red en Defensa de los Derechos Digitales, “Persisten interrogantes respecto de la información presentada por la SSPC sobre la adquisición y uso de Pegasus”, 29 de julio de 2021, disponible en: https://r3d.mx/2021/07/29/interrogantes-sspc-pegasus/

La impunidad también prevalece en otros casos de vigilancia ilegal, como el acceso ilegal a datos conservados por empresas de telecomunicaciones en perjuicio de la periodista Marcela Turati, la antropóloga forense Mercedes Doretti y la defensora de derechos humanos Ana Lorena Delgadillo, ni las decenas de personas cuyos datos fueron indebidamente accedidos por las Fiscalías de la Ciudad de México y Colima, simulando su relevancia para en investigaciones sobre secuestro.

No existe ninguna investigación abierta en torno al uso de herramientas de vigilancia masiva, como las antenas falsas o las herramientas de outsourcing de vigilancia masiva, ni el documentado uso ilegal de la herramienta de geolocalización *Geomatrix*, otras tecnologías de *spyware* como las desarrolladas por la empresa *Hacking Team*, ni se ha indagado sobre los indicios de utilización de herramientas de vigilancia de manera previa a los homicidios de los periodistas Cecilio Pineda Brito y Freddy Román Román.

La rampante impunidad por la corrupción en la adquisición de equipos y sistemas de vigilancia, por el espionaje ilegal a través de las mismas, así como por la conductas de encubrimiento y obstrucción de justicia ha generado un clima propicio para el abuso.

La ausencia absoluta de medidas que fomenten la prevención de abusos, la improbabilidad de la detección de los mismos y la prácticamente garantizada impunidad aún en los casos en los que irregularidades son detectadas demuestra que la vigilancia continúa fuera de control y que los casos de abuso se seguirán repitiendo y agravando si no se adoptan medidas profundas de reforma para establecer controles democráticos a la vigilancia de comunicaciones en México.

PROPUESTAS PARA EL ESTABLECIMIENTO DE CONTROLES DEMOCRÁTICOS A LA VIGILANCIA DE COMUNICACIONES

A partir del diagnóstico presentado, se considera indispensable el rediseño e implementación de una reforma profunda al marco jurídico e institucional en México, de manera que las facultades de vigilancia de comunicaciones en México —en cumplimiento de las recomendaciones y estándares internacionales— posean suficientes controles democráticos para prevenir, detectar y remediar abusos, evitar la corrupción y garantizar la verdad y justicia.

Frente a la evidencia del abuso generalizado y sistemático de la vigilancia en México, en el Informe conjunto del Relator Especial para la libertad de expresión de la CIDH y el Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión sobre su misión a México, publicado en Junio de 2018, se realizó la siguiente recomendación:

> *89. Los Relatores Especiales instan a las autoridades a adoptar las siguientes medidas:*
> *[...]*
> *(b) Establecer un marco legal para proteger a personas de intromisiones arbitrarias o clandestinas en su privacidad, incluida la protección de las fuentes periodísticas*

conforme a los estándares internacionales sobre la materia. Se deben establecer garantías y medidas de supervisión judicial de los organismos estatales implicados en vigilancia, dentro de los límites permisibles en una sociedad democrática. México debería considerar la posibilidad de crear un órgano independiente para supervisar de manera eficaz las tareas de vigilancia del Estado.

En este sentido, para la implementación de estas recomendaciones se proponen una serie de reformas que, adicionalmente a lo ya recomendado respecto de la adquisición de sistemas de vigilancia, persiguen tres objetivos fundamentales:

A. **Prevenir o evitar** el abuso de medidas de vigilancia.
B. **Detectar** el abuso de medidas de vigilancia.
C. **Sancionar y remediar** los abusos de medidas de vigilancia.

Para efectos de esta iniciativa, se entiende que las medidas de vigilancia incluyen la intervención de comunicaciones privadas, el acceso a datos conservados, la localización geográfica en tiempo real de dispositivos y la extracción de información de dispositivos.

a. Definición clara, precisa y detallada de las autoridades facultadas, el procedimiento y circunstancias en las que pueden llevarse a cabo medidas de vigilancia.

Con el objetivo de evitar la incertidumbre jurídica y la discrecionalidad en el despliegue de medidas de vigilancia, es necesario establecer con mayor explicitud aspectos fundamentales, como la identificación de las autoridades facultadas, la exclusividad de la competencia de la autoridad judicial federal para conocer de las solicitudes en la materia, así como delimitar y orientar con mayor precisión los parámetros y límites materiales que deben informar las solicitudes de autorización de medidas de vigilancia y las resoluciones judiciales que resuelven dichas solicitudes, garantizando así una mayor previsibilidad sobre los alcances de estas medidas.

Para ello, deben modificarse diversas disposiciones como el Código Nacional de Procedimientos Penales (CNPP), la Ley de Seguridad Nacional (LSN), la Ley de la Guardia Nacional (LGN), el Código Militar de Procedimientos Penales (CMPP), la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), la Ley Orgánica del Poder Judicial Federal (LOPJF) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), entre otras disposiciones, para establecer con claridad, precisión y detalle lo siguiente:

i. Debe **definirse con absoluta precisión y claridad qué autoridades se encuentran facultadas** para llevar a cabo medidas de vigilancia, **incluyendo aquéllas que no requieren colaboración de algún concesionario o proveedor**, así como los **casos y circunstancias en las que la autoridad judicial federal podrá autorizarlas**. Al hacerlo, deben observarse los límites subjetivos y materiales que establece el artículo 16 constitucional. Es decir,

únicamente pueden considerarse autoridades facultadas, aquéllas autoridades federales facultadas explícitamente por una ley, así como los titulares del Ministerio Público de cada entidad federativa; y no podrán autorizarse medidas de vigilancia relacionadas a materias carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

ii. Se debe reconocer de manera explícita que las medidas de vigilancia solamente podrán ser autorizadas por una **autoridad judicial federal** cuando sea una medida **idónea, necesaria y proporcional**. Lo anterior implica exigir, como mínimo, estándares probatorios mínimos que justifiquen la autorización de las medidas, como lo es el **estándar de "causa probable"**.

iii. Deben **prohibirse de manera expresa las medidas de vigilancia masiva** y las medidas de vigilancia que **comprometan masivamente la integridad y seguridad de sistemas de comunicación**.

b. Registro y control de proveedores de tecnologías de vigilancia

México carece de regulación efectiva de los procesos de adquisición de equipos y sistemas de vigilancia de comunicaciones. La ausencia de regulación de la industria que desarrolla y comercializa herramientas de vigilancia incrementa el riesgo de su adquisición por parte de entes no autorizados, facilita la discrecionalidad, los sobrecostos y la corrupción, exacerba los riesgos de despliegue de medidas de vigilancia ilegales y genera obstáculos para que las autoridades con facultades de supervisión e investigación lleven a cabo su crucial labor para prevenir, detectar y remediar abusos.

Por ello, se propone el establecimiento de las siguientes medidas:

i. Establecimiento de un registro de proveedores

Resulta indispensable establecer un registro de proveedores de equipos y sistemas de vigilancia de comunicaciones que permita contar con un control respecto de las personas que comercializan tecnologías de vigilancia. Este registro debe incluir datos de identificación del nombre o razón social del proveedor, datos de contacto, catálogo de equipos y sistemas de vigilancia de comunicaciones que el proveedor comercializa, datos de identificación del fabricante o desarrollador de los productos o servicios, así como el país de origen de los mismos.

Esta información resulta útil para que las autoridades facultadas para adquirir y desplegar medidas de vigilancia de comunicaciones puedan identificar potenciales proveedores y disminuir la discrecionalidad y el dispendio de recursos públicos. Así mismo, constituye información de suma relevancia para que autoridades con facultades de investigación, fiscalización y auditoría puedan indagar casos de abuso.

ii. Requisitos de inscripción orientados a garantizar la cooperación con investigaciones

Con el objetivo de evitar que, argumentando impedimentos legales o contractuales, algún proveedor argumente la imposibilidad de cooperar con investigaciones, resulta necesario establecer como requisito para la inscripción en el registro que los proveedores manifiesten la ausencia de impedimentos de esa naturaleza.

Este requisito, por un lado, permite garantizar la cooperación ante la investigación de potenciales abusos, pero también contribuye a incentivar que otras jurisdicciones en las que los equipos y sistemas de vigilancia son desarrollados modifiquen los impedimentos para dicha colaboración, ante el riesgo de que su industria se vea marginada de mercados importantes como el mexicano.

iii. Requisitos de inscripción orientados a proteger los derechos humanos

De manera similar a la propuesta anterior, el proceso de registro de proveedores ofrece una oportunidad para que México, en cumplimiento de su obligación de proteger derechos humanos, a la luz de los Principios Rectores sobre las Empresas y los Derechos Humanos, evite contribuir a violaciones a derechos humanos en las que proveedores de equipos y sistemas de vigilancia tengan alguna participación.

Para ello, la regulación debe establecer como impedimento para la inscripción en el registro de proveedores el que los mismos, así como sus subsidiarias y filiales o las personas fabricantes o desarrolladoras de los equipos y sistemas de vigilancia, comercialicen sus productos o servicios en países donde se cometan violaciones sistemáticas a los derechos humanos.

Para determinar lo anterior, sería deseable que alguna dependencia, como lo podría ser la Secretaría de Relaciones Exteriores o la Secretaría de Economía, mantenga una lista de personas físicas o morales que considere deben ser restringidas, de manera similar a como lo hace el Departamento de Comercio de los Estados Unidos[30].

iv. Requisitos de inscripción orientados a proteger la seguridad nacional

La adquisición de tecnologías avanzadas de vigilancia también pueden conllevar riesgos a la seguridad nacional, en tanto puede contener puertas traseras *(backdoors)* u otras características que permitan a una entidad extranjera explotar vulnerabilidades en perjuicio de los intereses legítimos de México.

---

[30] Departamento de Comercio de los Estados Unidos, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, 3 de noviembre de 2021. Disponible en: https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

El procedimiento de registro de proveedores ofrece una oportunidad para que el Estado mexicano pueda atender los riesgos a la seguridad nacional, señalando como impedimento para el registro que los proveedores, así como sus subsidiarias y filiales o las personas fabricantes o desarrolladoras de los equipos y sistemas de vigilancia, se considere que amenazan la seguridad nacional del país.

Para ello, es deseable utilizar el mismo mecanismo propuesto anteriormente, en el que alguna dependencia, como lo podría ser la Secretaría de Relaciones Exteriores, la Secretaría de Economía, el Centro Nacional de Inteligencia o el Consejo de Seguridad Nacional, mantenga una lista de personas físicas o morales que considere deben ser restringidas, de manera similar a como lo hace el Departamento de Comercio de los Estados Unidos o a través de órdenes ejecutivas por parte de la presidencia de los Estados Unidos[31].

c. Registro y control en los procesos de adquisición de equipos y sistemas de vigilancia

Los procesos de adquisición de equipos y sistemas de vigilancia deben regularse de manera específica con el objetivo de que dichas tecnologías no sean adquiridas de manera ilegal. Por ejemplo, al ser tecnologías con capacidades que exceden los principios de necesidad y proporcionalidad o al pretender ser adquiridas por entes no facultados. La estricta documentación de estos procedimientos también ofrece elementos para prevenir actos de corrupción y permitir la detección, investigación y sanción de cualquier irregularidad.

Para este fin, se propone establecer procedimientos en los que dentro de los requisitos previos a la adquisición de este tipo de tecnologías, se exija la obtención de una autorización por parte de alguna dependencia ajena a la contratación.

Dicha dependencia deberá asegurarse, por ejemplo, de que la autoridad contratante cuenta con facultades legales para llevar a cabo medidas de vigilancia; que los proveedores se encuentran registrados, cumplen con todos los requisitos y no se ubican en las causales de impedimento desarrolladas previamente; y que las tecnologías adquiridas cumplen con diversos parámetros para asegurar su legalidad y permitir la trazabilidad de su uso.

En este sentido, la regulación debe asegurarse de que la tecnología que pretende ser adquirida:

i. **No constituye una tecnología de vigilancia masiva**. Es decir, su despliegue únicamente afecta de manera focalizada al objetivo de vigilancia y no compromete masivamente la integridad y seguridad de los sistemas de comunicación.

---

[31] Oficina de la Presidencia de los Estados Unidos, Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, 27 de marzo de 2023. Disponible en: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

ii. **Es comercializada o desarrollada por una persona registrada en el registro de proveedores.** Incluyendo verificar que no existen impedimentos legales o contractuales para la colaboración con autoridades competentes para investigar conductas relacionadas al uso ilegal de los equipos o sistemas de vigilancia.

iii. **Es comercializada o desarrollada por una persona que no se encuentra incluída en la lista de personas impedidas**. Por ejemplo, por su participación en la comisión de violaciones graves a los derechos humanos o por constituir amenazas a la seguridad nacional.

iv. Posee mecanismos que garantizan la rendición de cuentas. Deben establecerse requisitos de diseño que incluyan medidas como los registros de auditoría inalterables, la inclusión de huellas digitales (*fingerprinting*) y otros mecanismos de seguridad que permitan detectar, trazar e investigar los usos de la tecnología.

Adicionalmente, la regulación debe establecer un registro de equipos y sistemas tecnológicos de vigilancia que contenga información que identifique a las dependencias que cuentan con estas herramientas, los proveedores y desarrolladores, los nombres comerciales de las mismas, las fechas de contratación, su vigencia, entre otra información relevante.

Para ello, se sugiere la inclusión de información sobre los equipos y sistemas tecnológicos de vigilancia adquiridos y utilizados por las autoridades competentes en el Registro Nacional de Armamento y Equipo al que se refiere el artículo 154 de la Ley General del Sistema Nacional de Seguridad Pública o en otro registro incorporado a una ley o disposición administrativa.

La existencia de este registro es crucial para permitir que las autoridades competentes para investigar, fiscalizar y auditar la adquisición y uso de estos sistemas, cuente con elemento suficientes para llevar a cabo su labor, inhibiendo así casos de abuso y permitiendo, en todo caso, su detección, investigación y sanción.

d. Registro y control del despliegue de medidas de vigilancia

En cumplimiento de las obligaciones constitucionales y legales existentes que disponen la existencia de registros de las medidas de vigilancia llevadas a cabo, es necesario establecer mecanismos de control y registro sobre el uso de medidas de vigilancia, de manera que queden asentadas de manera pormenorizada e inmutable las medidas de vigilancia encubierta que sean llevadas a cabo por las autoridades competentes.

En concreto se sugiere establecer:

i. Requisitos e identificación de agentes que participan en la toma de decisiones y operación de sistemas de vigilancia: Establecer requisitos de certificación, evaluaciones de control de confianza y mantener un registro pormenorizado de los agentes que hayan sido capacitados y que participen en la implementación de medidas de vigilancia.

ii. **Registros de uso:** Establecer mecanismos que garanticen el registro pormenorizado de la utilización de medidas de vigilancia, incluyendo los agentes participantes, los sujetos, métodos utilizados y otros datos necesarios para identificar cada uso de medidas de vigilancia.
iii. **Mecanismos para prevenir el uso no registrado de sistemas de vigilancia o la alteración del registro:** Establecer la obligación de implementar medidas técnicas y administrativas para prevenir usos no registrados de sistemas de vigilancia o alteraciones en el registro de uso.

e. Control judicial efectivo

Con el objetivo de garantizar la efectividad del control judicial sobre las medidas de vigilancia, es indispensable fortalecer las medidas de control judicial existentes de la siguiente manera:

i. **Exclusiva competencia federal:** A partir de los precedentes judiciales que así lo han establecido, resulta necesario armonizar la legislación, por ejemplo el artículo 303 del CNPP, para establecer de manera inequívoca que únicamente la autoridad judicial federal es competente para conocer y resolver de solicitudes de autorización de medidas de vigilancia, incluyendo el acceso a datos conservados y la localización geográfica en tiempo real.
ii. **Registro de control judicial:** Establecer mecanismos que garanticen el registro pormenorizado de medidas de vigilancia cuya autorización es solicitada u otorgada por el Poder Judicial de la Federación, incluyendo las autoridades solicitantes, los sujetos, los métodos, sistemas o herramientas utilizadas, en su caso, los concesionarios, autorizados o proveedores que deban prestar alguna colaboración y otros datos necesarios para identificar cada uso de medidas de vigilancia.
iii. **Modificación del mecanismo excepcional establecido en el artículo 303 del CNPP:** Es necesario reformular los mecanismos de emergencia contemplados en el CNPP, de manera que la solicitud de ratificación de medidas de vigilancia deba ser enviada al Juez de Control competente de manera simultánea a cualquier requerimiento a un concesionario, autorizado o proveedor, o al inicio de la medida misma. Igualmente, debe establecerse el procedimiento a seguir cuando la orden de ratificación sea negada, el cual debe incluir la notificación a la persona afectada y procedimientos disciplinarios adecuados.
iv. **Supervisión de las medidas:** Es necesario fortalecer las capacidades de supervisión de medidas de vigilancia autorizadas por parte de la autoridad judicial que otorgue dicha autorización. Para ello es necesario contemplar mecanismos técnicos y administrativos que permitan que dicha supervisión sea desarrollada de manera autónoma, inclusive sin necesidad de cooperación o conocimiento de parte de la autoridad que lleva a cabo las medidas de vigilancia. Por ejemplo, permitiendo a la autoridad judicial el acceso autónomo a los registros de auditoría de las herramientas de vigilancia utilizadas.

f. Reconocimiento del derecho de notificación

Con el objeto de inhibir instancias de abuso y garantizar que las personas afectadas por medidas de vigilancia cuentan con la posibilidad de ejercer su derecho de acceso a la justicia, es necesario reconocer el derecho de notificación de las personas que son objeto de medidas de vigilancia. Es decir, la obligación de parte de la autoridad de notificar a una persona que su privacidad o datos personales fueron interferidos mediante una medida de vigilancia encubierta.

Si bien, como es establecido en el derecho comparado, dicha notificación puede no poder llevarse a cabo de manera previa o inmediata, en tanto se podría obstaculizar el éxito de una investigación legítima, dicha notificación puede llevarse a cabo de manera diferida, cuando no esté en riesgo una investigación, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento pueda generar un riesgo inminente de peligro a la vida o integridad personal de alguna persona.

En concreto se propone:

i. Regular la **obligación de notificar** a las personas que hayan sido sujetas a una medida de vigilancia.
ii. Establecer el **control judicial de este proceso y la posibilidad de diferir la notificación**, por un tiempo determinado, cuando sea necesario para evitar el peligro de fuga, la destrucción de evidencia o un riesgo inminente a la vida o integridad de una persona.
iii. Se debe establecer la **obligación de colaboración** de parte de concesionarios y autorizados para prestar servicios de telecomunicaciones, así como a proveedores de aplicaciones, contenidos y servicios en Internet respecto de la colaboración con autoridades de seguridad y justicia para llevar a cabo la notificación correspondiente.
iv. La **notificación debe incluir información relevante** como la autoridad que llevo a cabo la medida, su duración, así como acceso a la información que fue obtenida.

g. Fortalecimiento de las facultades de fiscalización, auditoría y supervisión independiente de medidas de vigilancia

En concordancia con la experiencia internacional, se propone el establecimiento de un mecanismo de supervisión independiente a las tareas de vigilancia de comunicaciones, mediante la creación de un órgano de supervisión independiente o en su defecto el desarrollo de dichas facultades dentro del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) o el órgano que le sustituya en sus facultades. En concreto se sugiere:

i. Otorgar facultades al órgano supervisor independiente para realizar **procedimientos de vigilancia, auditoría o verificación oficiosa**, incluyendo de manera aleatoria, para verificar el cumplimiento de las disposiciones que regulan las medidas de vigilancia.
ii. Reconocer explícitamente la **facultad de acceder y requerir a cualquier autoridad cualquier información** necesaria para llevar a cabo su función de supervisión, incluyendo información reservada. También debe incluirse la facultad de requerir información a particulares que presten colaboración a autoridades para llevar a cabo medidas de vigilancia encubierta.
iii. Establecer la obligación de producir un **informe periódico y público** sobre los hallazgos y recomendaciones del órgano supervisor.

h. Transparencia efectiva

A partir del diagnóstico presentado, es necesario adoptar disposiciones que permitan contar con medidas de transparencia efectiva para prevenir, detectar y remediar instancias de abuso. Para ello, es necesario contar con información estadística con suficiente granularidad y comparabilidad de manera que sea posible evaluar la efectividad de las medidas y detectar posibles irregularidades.

Igualmente, es necesario garantizar el acceso a información suficiente sobre los equipos y sistemas de vigilancia utilizados y sobre los procesos de autorización de las medidas, de manera que la sociedad pueda conocer y evaluar de manera general el alcance y pertinencia de las medidas de vigilancia y de las normas que las regulan.

i. Reformas legales en materia de transparencia

Resulta útil llevar a cabo reformas que hagan explícitos los precedentes de interpretación administrativa y judicial vigentes relacionados a la vigilancia de comunicaciones.

Por ejemplo, sería deseable mejorar la redacción de la fracción XLVII del artículo 70 de la LGTAIP, para establecer con mayor claridad los sujetos obligados y el nivel de desagregación que debe ser reportado como parte de las obligaciones de transparencia oficiosa.

Igualmente, sería ideal realizar otras reformas a la Ley Federal de Telecomunicaciones y Radiodifusión, al Código Nacional de Procedimientos Penales, la Ley de Seguridad Nacional, la Ley de la Guardia Nacional, entre otras, para explicitar, cómo ha sido interpretado por la SCJN que no pueden invocarse disposiciones en dichos ordenamientos para impedir de manera absoluta y automática el acceso a la información en las materias de procuración de justicia, seguridad pública o seguridad nacional, sin atenerse a los principios de transparencia y acceso a la información pública establecidos en la LGTAIP, especialmente cuando existen indicios de posibles violaciones a derechos humanos o actos de corrupción.

Un objetivo fundamental de las reformas debe consistir en garantizar que existan diversas fuentes de información estadística sobre las medidas de vigilancia, estableciendo que tanto las autoridades facultadas para solicitar su autorización y ejecutarlas, como el Poder Judicial Federal, encargado de analizar y, en su caso, autorizar y supervisar las medidas y las empresas que, en su caso, colaboren en la ejecución de las medidas de vigilancia, deban publicar información estadística.

Es fundamental que la información estadística publicada por los diversos sujetos obligados sea comparable entre sí, para ello, deben establecerse las mismas categorías de datos estadísticos a ser recabados y publicados y en la misma periodicidad. De esta manera, será posible detectar anomalías que conlleven a la investigación de probables abusos.

De manera concreta se proponen las siguientes reformas:

A. Código Nacional de Procedimientos Penales

CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES VIGENTE	PROPUESTA DE REFORMA
Artículo 218. Reserva de los actos de investigación Los registros de la investigación, así como todos los documentos, independientemente de su contenido o naturaleza, los objetos, los registros de voz e imágenes o cosas que le estén relacionados, son estrictamente reservados, por lo que únicamente las partes, podrán tener acceso a los mismos, con las limitaciones establecidas en este Código y demás disposiciones aplicables. La víctima u ofendido y su Asesor Jurídico podrán tener acceso a los registros de la investigación en cualquier momento. El imputado y su defensor podrán tener acceso a ellos cuando se encuentre detenido, sea citado para comparecer como imputado o sea sujeto de un acto de molestia y se pretenda recibir su entrevista, a partir de este momento ya no podrán mantenerse en reserva los registros para el imputado o su Defensor a fin de no afectar su derecho de defensa. Para los efectos de este párrafo, se entenderá como acto de molestia lo dispuesto en el artículo 266 de este Código.	**Artículo 218. Reserva de los actos de investigación** Los registros de la investigación, así como todos los documentos, independientemente de su contenido o naturaleza, los objetos, los registros de voz e imágenes o cosas que le estén relacionados, son estrictamente reservados, por lo que únicamente las partes, podrán tener acceso a los mismos, con las limitaciones establecidas en este Código y demás disposiciones aplicables. La víctima u ofendido y su Asesor Jurídico podrán tener acceso a los registros de la investigación en cualquier momento. El imputado y su defensor podrán tener acceso a ellos cuando se encuentre detenido, sea citado para comparecer como imputado o sea sujeto de un acto de molestia y se pretenda recibir su entrevista, a partir de este momento ya no podrán mantenerse en reserva los registros para el imputado o su Defensor a fin de no afectar su derecho de defensa. Para los efectos de este párrafo, se entenderá como acto de molestia lo dispuesto en el artículo 266 de este Código.

En ningún caso la reserva de los registros podrá hacerse valer en perjuicio del imputado y su Defensor, una vez dictado el auto de vinculación a proceso, salvo lo previsto en este Código o en las leyes especiales. Para efectos de acceso a la información pública gubernamental, el Ministerio Público únicamente deberá proporcionar una versión pública de las determinaciones de no ejercicio de la acción penal, archivo temporal o de aplicación de un criterio de oportunidad, siempre que haya transcurrido un plazo igual al de prescripción de los delitos de que se trate, de conformidad con lo dispuesto en el Código Penal Federal o estatal correspondiente, sin que pueda ser menor de tres años, ni mayor de doce años, contado a partir de que dicha determinación haya quedado firme.	En ningún caso la reserva de los registros podrá hacerse valer en perjuicio del imputado y su Defensor, una vez dictado el auto de vinculación a proceso, salvo lo previsto en este Código o en las leyes especiales. **Nada de lo señalado en este Código deberá obstaculizar el ejercicio de las facultades de supervisión, fiscalización o investigación, llevadas a cabo por las autoridades competentes, respecto de las responsabilidades administrativas o penales en que incurran los funcionarios públicos que lleven a cabo actos de investigación. Tampoco obstaculizará el derecho de acceso a la información en los términos establecidos por la Ley Federal de Transparencia y Acceso a la Información Pública.** ~~**Para efectos de acceso a la información pública gubernamental, el Ministerio Público únicamente deberá proporcionar una versión pública de las determinaciones de no ejercicio de la acción penal, archivo temporal o de aplicación de un criterio de oportunidad, siempre que haya transcurrido un plazo igual al de prescripción de los delitos de que se trate, de conformidad con lo dispuesto en el Código Penal Federal o estatal correspondiente, sin que pueda ser menor de tres años, ni mayor de doce años, contado a partir de que dicha determinación haya quedado firme.**~~
Artículo 291. Intervención de las comunicaciones privadas Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Procuraduría General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.	**Artículo 291. Intervención de las comunicaciones privadas** Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la ~~**Procuraduría**~~ **Fiscalía** General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.

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. La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos. Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.	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. La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. También se requerirá autorización judicial **federal** en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos. Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.
Artículo 292. Requisitos de la solicitud La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención.	**Artículo 292. Requisitos de la solicitud** La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones **o la empresa prestadora de servicios, aplicaciones o contenidos en**

El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.	**Internet a través del cual se realiza la comunicación objeto de la intervención, así como la tecnología** a través del cual se realiza la comunicación objeto de la intervención. El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.
Artículo 293. Contenido de la resolución judicial que autoriza la intervención de las comunicaciones privadas En la autorización, el Juez de control determinará las características de la intervención, sus modalidades, límites y en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración.	**Artículo 293. Contenido de la resolución judicial que autoriza la intervención de las comunicaciones privadas** En la autorización, el Juez de control **federal analizará la idoneidad, necesidad y proporcionalidad de la intervención y** determinará las características de la ~~**intervención**~~ **misma**, sus modalidades, límites y en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración. **No se autorizarán intervenciones o el empleo de tecnologías o métodos de colaboración que constituyan medidas de vigilancia masiva o indiscriminada, comprometan de manera masiva la seguridad e integridad de los sistemas de comunicación o que no permitan al Juez hacer las verificaciones a las que se refiere el artículo 294.**
Artículo 299. Conclusión de la intervención Al concluir la intervención, la Policía o el perito, de manera inmediata, informará al Ministerio Público sobre su desarrollo, así como de sus resultados y levantará el acta respectiva. A su vez, con la misma prontitud el Ministerio Público que haya solicitado la intervención o su prórroga lo informará al Juez de control.	**Artículo 299. Conclusión de la intervención** Al concluir la intervención, la Policía o el perito, de manera inmediata, informará al Ministerio Público sobre su desarrollo, así como de sus resultados y levantará el acta respectiva. A su vez, con la misma prontitud el Ministerio Público que haya solicitado la intervención o su prórroga lo informará al Juez de control. **Tras la conclusión de la intervención, el juez de control ordenará que las personas objeto de la intervención sean notificadas de conformidad con lo que señala esta Ley y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.** **Cuando sea necesario para evitar el peligro de fuga, destrucción de evidencia o se ponga en riesgo la investigación o la vida o integridad**

	de una persona, la notificación podrá prorrogarse por un plazo no mayor a seis meses posterior a la conclusión de la intervención, previa autorización del juez que autorizó la misma.
Artículo 300. Destrucción de los registros El Órgano jurisdiccional ordenará la destrucción de aquellos registros de intervención de comunicaciones privadas que no se relacionen con los delitos investigados o con otros delitos que hayan ameritado la apertura de una investigación diversa, salvo que la defensa solicite que sean preservados por considerarlos útiles para su labor. Asimismo, ordenará la destrucción de los registros de intervenciones no autorizadas o cuando éstos rebasen los términos de la autorización judicial respectiva. Los registros serán destruidos cuando se decrete el archivo definitivo, el sobreseimiento o la absolución del imputado. Cuando el Ministerio Público decida archivar temporalmente la investigación, los registros podrán ser conservados hasta que el delito prescriba.	**Artículo 300. Destrucción de los registros** El Órgano jurisdiccional ordenará la destrucción de aquellos registros de intervención de comunicaciones privadas que no se relacionen con los delitos investigados o con otros delitos que hayan ameritado la apertura de una investigación diversa, salvo que la defensa solicite que sean preservados por considerarlos útiles para su labor. Asimismo, ordenará la destrucción de los registros de intervenciones no autorizadas o cuando éstos rebasen los términos de la autorización judicial respectiva. Los registros serán destruidos cuando se decrete el archivo definitivo, el sobreseimiento o la absolución del imputado. Cuando el Ministerio Público decida archivar temporalmente la investigación, los registros podrán ser conservados hasta que el delito prescriba. **La destrucción de los registros no podrá realizarse hasta que la persona afectada haya sido notificada en términos de lo que señala esta Ley y la Ley General de Protección de Datos en Posesión de Sujetos Obligados.**
Artículo 301. Colaboración con la autoridad Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con las disposiciones aplicables. Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas. El incumplimiento a este mandato será sancionado conforme a las disposiciones penales aplicables.	**Artículo 301. Colaboración con la autoridad** Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con **la autorización judicial federal que las ordene y** las disposiciones aplicables. Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas. El incumplimiento a este mandato será sancionado conforme a las disposiciones penales aplicables.
Artículo 303. Localización geográfica en	**Artículo 303. Localización geográfica en**

tiempo real y solicitud de entrega de datos conservados Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente. En la solicitud se expresarán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida. La petición deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público. Si la resolución se emite o registra por medios diversos al escrito, los puntos resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público. En caso de que el Juez de control niegue la orden de localización geográfica en tiempo real o la entrega de los datos conservados, el Ministerio Público podrá subsanar las deficiencias y solicitar nuevamente la orden o podrá apelar la decisión. En este caso la apelación debe ser resuelta en un plazo no mayor de doce horas a partir de que se	**tiempo real y solicitud de entrega de datos conservados** Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o la entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control **federal competente ~~del fuero correspondiente~~ la autorización para llevar a cabo dichos actos de investigación y,** en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente **previa notificación a la persona afectada en términos de lo que señala esta Ley y la Ley General de Protección de Datos en Posesión de Sujetos Obligados.** En la solicitud se expresarán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida**, así como la tecnología empleada para llevar a cabo la intervención**. La petición deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público. **Sin perjuicio de lo anterior, el Juez analizará la idoneidad, necesidad y proporcionalidad del requerimiento y determinará las características del mismo, sus modalidades, límites y en su caso, ordenará a instituciones**

interponga. Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria. A partir de que se haya cumplimentado el requerimiento, el Ministerio Público deberá informar al Juez de control competente por cualquier medio que garantice su autenticidad, dentro del plazo de cuarenta y ocho horas, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación. Cuando el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al procedimiento penal. Asimismo el Procurador, o el servidor público en quien se delegue la facultad podrá requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. La solicitud y entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por este artículo. Lo anterior sin menoscabo de las obligaciones previstas en materia de conservación de información para las concesionarias y autorizados de telecomunicaciones en términos del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión.	**públicas o privadas modos específicos de colaboración.** **No se autorizarán requerimientos o el empleo de tecnologías o métodos de colaboración que constituyan medidas de vigilancia masiva o indiscriminada, comprometan de manera masiva la seguridad e integridad de los sistemas de comunicación o que no permitan al Juez hacer las verificaciones a las que se refiere esta Ley.** Si la resolución se emite o registra por medios diversos al escrito, los puntos resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público. En caso de que el Juez de control niegue la ~~**orden**~~ **autorización** de localización geográfica en tiempo real o la entrega de los datos conservados, el Ministerio Público podrá subsanar las deficiencias y solicitar nuevamente la ~~**orden**~~ **autorización** o podrá apelar la decisión. En este caso la apelación debe ser resuelta en un plazo no mayor de doce horas a partir de que se interponga. Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria. A partir de que se haya ~~**cumplimentado**~~ **formulado** el requerimiento, el Ministerio Público deberá informar al Juez de control **federal** competente por cualquier medio que garantice su autenticidad, **de manera inmediata** ~~**dentro del plazo de cuarenta y ocho horas**~~, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación. Cuando el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al

	procedimiento penal **y se procederá a la notificación correspondiente a la persona afectada en términos de lo que señala esta Ley y la Ley General de Protección de Datos en Posesión de Sujetos Obligados** . Asimismo el Procurador, o el servidor público en quien se delegue la facultad podrá requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. La solicitud y entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por este artículo. Lo anterior sin menoscabo de las obligaciones previstas en materia de conservación de información para las concesionarias y autorizados de telecomunicaciones en términos del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión.

B. Ley de la Guardia Nacional

LEY DE LA GUARDIA NACIONAL VIGENTE	PROPUESTA DE REFORMA
Artículo 100. De conformidad con los artículos 16 y 21 de la Constitución Política de los Estados Unidos Mexicanos, con la Ley Federal Contra la Delincuencia Organizada, con la Ley de Seguridad Nacional, con el Código Nacional de Procedimientos Penales, y con la presente Ley, la Guardia Nacional podrá solicitar la intervención de comunicaciones. La autorización judicial correspondiente podrá otorgarse a solicitud del Comandante o del titular de la Jefatura General de Coordinación Policial, cuando se constatare la existencia de indicios suficientes que acrediten que se está organizando la comisión de los delitos que se señalan en el artículo 103 de esta Ley. En caso de que durante la intervención de comunicaciones se advierta el indicio de la posible comisión de un hecho delictivo, se hará del conocimiento inmediato al Ministerio Público.	Artículo 100. De conformidad con los artículos 16 y 21 de la Constitución Política de los Estados Unidos Mexicanos, con la Ley Federal Contra la Delincuencia Organizada, con la Ley de Seguridad Nacional, con el Código Nacional de Procedimientos Penales, **la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados** y con la presente Ley, la Guardia Nacional podrá ~~**solicitar**~~ **llevar a cabo** la intervención de comunicaciones**, el acceso a datos conservados y la georreferenciación de equipos de comunicación móvil previa autorización judicial federal**. La autorización judicial correspondiente podrá otorgarse a solicitud del Comandante o del titular de la Jefatura General de Coordinación Policial, cuando se constatare la existencia de indicios suficientes que acrediten que se está organizando la comisión de los delitos que se señalan en el artículo 103 de esta Ley.

	En caso de que durante la intervención de comunicaciones se advierta el indicio de la posible comisión de un hecho delictivo, se hará del conocimiento inmediato al Ministerio Público.
Artículo 102. Los servidores públicos autorizados para la ejecución de las intervenciones serán responsables de que se realicen en los términos de la resolución judicial. La solicitud de autorización 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, el cual podrá ser prorrogado bimestralmente sin que el periodo de intervención, incluyendo sus prórrogas, pueda exceder de seis meses. Después de dicho plazo, solo podrán autorizarse nuevas intervenciones cuando el Secretario o el Comandante acrediten nuevos elementos que así lo justifiquen. En su autorización, la autoridad judicial competente determinará las características de la intervención, sus modalidades y límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.	Artículo 102. Los servidores públicos autorizados para la ejecución de las intervenciones serán responsables de que se realicen en los términos de la resolución judicial. La solicitud de autorización 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, **el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionaria del servicio de telecomunicaciones o la empresa prestadora de servicios, aplicaciones o contenidos en Internet a través del cual se realiza la comunicación objeto de la intervención, así como la tecnología empleada para llevar a cabo la intervención,** así como el periodo durante el cual se llevarán a cabo las intervenciones, el cual podrá ser prorrogado bimestralmente sin que el periodo de intervención, incluyendo sus prórrogas, pueda exceder de seis meses. Después de dicho plazo, solo podrán autorizarse nuevas intervenciones cuando el Secretario o el Comandante acrediten nuevos elementos que así lo justifiquen. En su autorización, la autoridad judicial competente **analizará la idoneidad, necesidad y proporcionalidad de la intervención y** determinará las características de la **misma** ~~**intervención**~~, sus modalidades y límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración. **No se podrán autorizar intervenciones o el empleo de tecnologías o métodos de colaboración que constituyan medidas de vigilancia masiva o indiscriminada, comprometan de manera masiva la seguridad e integridad de los sistemas de comunicación o que no permitan al Juez hacer las verificaciones a las que se refiere el artículo 104.**
Artículo 104. En la autorización judicial que se otorgue para la ejecución de las intervenciones,	Artículo 104. En la autorización judicial que se otorgue para la ejecución de las intervenciones,

deberá ordenarse que, cuando en la misma práctica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá presentar ante la autoridad judicial competente una nueva solicitud. También se ordenará en ella que, al concluir cada intervención, se levante un acta que contenga un inventario pormenorizado de la información de audio o video con los sonidos o imágenes captados durante la intervención, y se entregue a la autoridad judicial un informe sobre los resultados de la intervención, a efecto de constatar el debido cumplimiento de la autorización otorgada. La autoridad judicial competente podrá, en cualquier momento, verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total. La autoridad judicial competente deberá acordar la solicitud en un plazo no mayor de doce horas a partir de su presentación. Independientemente de lo anterior, la Guardia Nacional deberá rendir un informe sobre la intervención que la autoridad judicial competente pondrá a disposición del Ministerio Público.	deberá ordenarse que, cuando en la misma práctica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá presentar ante la autoridad judicial **federal** competente una nueva solicitud. También se ordenará en ella que, al concluir cada intervención, se levante un ~~**acta**~~ **registro** que contenga **las fechas de inicio y término de la intervención,** un inventario pormenorizado de **toda información recabada, incluyendo** la información de audio o video con los sonidos o imágenes captados durante la intervención,**cuando no se ponga en riesgo a la investigación o a la persona, la identificación de quienes hayan participado en los actos de investigación, así como los demás datos que se consideren relevantes para la investigación. El registro original y el duplicado, así como los documentos que los integran, se numerarán progresivamente y contendrán los datos necesarios para su identificación.** ~~**y**~~ **Además se ordenará que** se entregue a la autoridad judicial un informe sobre los resultados de la intervención, a efecto de constatar el debido cumplimiento de la autorización otorgada. La autoridad judicial **federal** competente podrá, en cualquier momento, verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total. La autoridad judicial **federal** competente deberá acordar la solicitud en un plazo no mayor de doce horas a partir de su presentación. Independientemente de lo anterior, la Guardia Nacional deberá rendir un informe sobre la intervención que la autoridad judicial competente pondrá a disposición del Ministerio Público. **Tras la conclusión de la intervención, el Órgano jurisdiccional ordenará que las personas objeto de la intervención sean notificadas de conformidad con lo que señala la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.** **Cuando sea necesario para evitar un riesgo inminente a la seguridad pública o a la vida o integridad de una persona, la notificación podrá prorrogarse por un plazo no mayor a**

	seis meses posterior a la conclusión de la intervención, previa autorización del juez que autorizó la misma.
Artículo 105. En caso de que la autoridad judicial competente que haya autorizado la intervención, concluya que de la investigación no existen elementos para que el caso sea conocido por el Ministerio Público, por no tratarse de conductas delictivas, ordenará que se ponga a su disposición la información resultado de las intervenciones y ordenará su destrucción en presencia del Comandante o del titular de la Jefatura General de Coordinación Policial. El Comandante o el titular de la Jefatura General de Coordinación Policial, bajo su estricta responsabilidad, garantizarán la reserva de las intervenciones de comunicaciones privadas que les hayan sido autorizadas y, en caso de incumplimiento, será sancionado penalmente. En caso de que durante la investigación preventiva se advierta la comisión de un delito, se dará vista de inmediato al Ministerio Público.	Artículo 105. En caso de que la autoridad judicial **federal** competente que haya autorizado la intervención, concluya que de la investigación no existen elementos para que el caso sea conocido por el Ministerio Público, por no tratarse de conductas delictivas, ordenará que se ponga a su disposición la información resultado de las intervenciones y ordenará su destrucción en presencia del Comandante o del titular de la Jefatura General de Coordinación Policial**, previa notificación de la intervención a la persona objeto de la misma, en los términos que señala el artículo 104 y la Ley General de Protección de Datos en Posesión de Sujetos Obligados.** El Comandante o el titular de la Jefatura General de Coordinación Policial, bajo su estricta responsabilidad, garantizarán la reserva de las intervenciones de comunicaciones privadas que les hayan sido autorizadas y, en caso de incumplimiento, será sancionado penalmente. En caso de que durante la investigación preventiva se advierta la comisión de un delito, se dará vista de inmediato al Ministerio Público. **Nada de lo señalado en esta Ley deberá obstaculizar el ejercicio de las facultades de supervisión, fiscalización o investigación, llevadas a cabo por las autoridades competentes, respecto de las responsabilidades administrativas o penales en que incurran los funcionarios públicos que lleven a cabo las intervenciones. Tampoco obstaculizará el derecho de acceso a la información en los términos establecidos por la Ley Federal de Transparencia y Acceso a la Información Pública.**

C. Ley de Seguridad Nacional

LEY DE SEGURIDAD NACIONAL VIGENTE	PROPUESTA DE REFORMA

Artículo 8.- A falta de previsión expresa en la presente Ley, se estará a las siguientes reglas de supletoriedad: (...) IV. En materia de coadyuvancia y de intervención de comunicaciones privadas, será aplicable el Código Federal de Procedimientos Penales y la Ley Federal contra la Delincuencia Organizada; (...)	Artículo 8.- A falta de previsión expresa en la presente Ley, se estará a las siguientes reglas de supletoriedad: (...) IV. En materia de coadyuvancia y de intervención de comunicaciones privadas, será aplicable el Código ~~Federal~~ **Nacional** de Procedimientos Penales**, la Ley General de Protección de Datos en Posesión de Sujetos Obligados, la Ley Federal de Telecomunicaciones y Radiodifusión** y la Ley Federal contra la Delincuencia Organizada; (...)
Artículo 34.- De conformidad con lo dispuesto por el párrafo noveno del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro deberá solicitar en los términos y supuestos previstos por la presente Ley, autorización judicial para efectuar intervenciones de comunicaciones privadas en materia de Seguridad Nacional. 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.	Artículo 34.- De conformidad con lo dispuesto por el párrafo ~~noveno~~ **décimo tercero** del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro deberá solicitar en los términos y supuestos previstos por la presente Ley, autorización judicial **federal** para efectuar intervenciones de comunicaciones privadas en materia de Seguridad Nacional. 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. **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.** **También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos**

	de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos.
Artículo 35.- La solicitud a que se refiere el artículo anterior sólo procederá cuando se esté en uno de los supuestos que se contemplan en el artículo 5 de la presente Ley. En ningún otro caso podrá autorizarse al Centro la intervención de comunicaciones privadas. El Poder Judicial de la Federación, de acuerdo con su ley orgánica, determinará los juzgados que deban conocer de las solicitudes que en materia de Seguridad Nacional se presenten para intervenir comunicaciones privadas.	Artículo 35.- La solicitud a que se refiere el artículo anterior sólo procederá cuando **se constate la existencia de indicios suficientes que acrediten que se está organizando la comisión de actos comprendidos dentro ~~se esté en uno~~** de los supuestos que se contemplan en el artículo 5 de la presente Ley. En ningún otro caso podrá autorizarse al Centro la intervención de comunicaciones privadas. El Poder Judicial de la Federación, de acuerdo con su ley orgánica, determinará los juzgados que deban conocer de las solicitudes que en materia de Seguridad Nacional se presenten para intervenir comunicaciones privadas.
Artículo 36.- Los procedimientos judiciales que se instauren para autorizar las solicitudes de intervención en materia de Seguridad Nacional no tendrán naturaleza contenciosa y sus constancias procesales carecerán de valor probatorio en procedimientos judiciales o administrativos. Cuando el Centro coopere en las actividades de procuración de justicia, las intervenciones de comunicaciones privadas en las que se preste auxilio técnico tendrán naturaleza distinta a las reguladas por este Capítulo y se ajustarán a los requisitos y formalidades que establezca el Código Federal de Procedimientos Penales y la Ley Federal contra la Delincuencia Organizada.	Artículo 36.- Los procedimientos judiciales que se instauren para autorizar las solicitudes de intervención en materia de Seguridad Nacional no tendrán naturaleza contenciosa y sus constancias procesales carecerán de valor probatorio en procedimientos judiciales o administrativos. Cuando el Centro coopere en las actividades de procuración de justicia, las intervenciones de comunicaciones privadas en las que se preste auxilio técnico tendrán naturaleza distinta a las reguladas por este Capítulo y se ajustarán a los requisitos y formalidades que establezca el Código **~~Federal~~ Nacional** de Procedimientos Penales y la Ley Federal contra la Delincuencia Organizada.
Artículo 37.- El procedimiento tiene carácter reservado, por lo que las solicitudes se registrarán en un libro de gobierno especial que se manejará	**Artículo 37.-** El procedimiento tiene carácter reservado, por lo que las solicitudes se registrarán en un libro de gobierno especial que se manejará

por el personal que para tal efecto designe el juez. No se permitirá el acceso a los expedientes a persona alguna, salvo al secretario del juzgado y a quien se autorice por escrito por parte del Director General del Centro.	por el personal que para tal efecto designe el juez. No se permitirá el acceso a los expedientes a persona alguna, salvo al secretario del juzgado y a quien se autorice por escrito por parte del Director General del Centro. **El libro a que se refiere el artículo anterior contendrá las fechas de inicio y término de la intervención, un inventario pormenorizado de los documentos, objetos y los medios para la reproducción de sonidos o imágenes captadas durante la misma, cuando no se ponga en riesgo a la investigación o a la persona, la identificación de quienes hayan participado en los actos de investigación, así como los demás datos a que se refieren los artículos 38 y 40 de la Ley. El registro original y el duplicado, así como los documentos que los integran, se numerarán progresivamente y contendrán los datos necesarios para su identificación.**
Artículo 38.- La solicitud a que se refiere el artículo 34 debe contener: I. Una descripción detallada de los hechos y situaciones que representen alguna amenaza para la Seguridad Nacional en los términos del artículo 5 de esta Ley. Dicha descripción omitirá datos de identificación de personas, lugares o cosas cuya difusión indebida, ponga en riesgo su seguridad o la investigación en curso. No obstante lo dispuesto en el párrafo anterior, los datos de identificación omitidos en la solicitud, serán presentados en un sobre cerrado, relacionado con la solicitud que acompaña, el cual será debidamente identificado y señalado por el juez mediante acuerdo reservado que recaiga a la solicitud. El expediente que se forma con este motivo, se manejará en sigilo y se guardará en el secreto del juzgado; II. Las consideraciones que motivaran la solicitud, y III. El lapso de vigencia de la autorización que	Artículo 38.- La solicitud a que se refiere el artículo 34 debe contener: I. Una descripción detallada de los hechos y situaciones que representen alguna amenaza para la Seguridad Nacional en los términos del artículo 5 de esta Ley. Dicha descripción omitirá datos de identificación de personas, lugares o cosas cuya difusión indebida, ponga en riesgo su seguridad o la investigación en curso. No obstante lo dispuesto en el párrafo anterior, los datos de identificación omitidos en la solicitud, serán presentados en un sobre cerrado, relacionado con la solicitud que acompaña, el cual será debidamente identificado y señalado por el juez mediante acuerdo reservado que recaiga a la solicitud. El expediente que se forma con este motivo, se manejará en sigilo y se guardará en el secreto del juzgado; II. Las consideraciones que motivara**ra**n la solicitud, y III. El lapso de vigencia de la autorización que

se solicita.	se solicita. **IV. La solicitud de intervención deberá precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionaria del servicio de telecomunicaciones o la empresa prestadora de servicios, aplicaciones o contenidos en Internet a través de la cual se realiza la comunicación objeto de la intervención, así como la tecnología empleada para llevar a cabo la intervención.**
Artículo 39.- Una vez presentada la solicitud, el juez debe proporcionar acuse de recibo y emitir dentro de las veinticuatro horas contadas a partir de la solicitud, una resolución fundada y motivada en la que puede otorgar o negar la autorización solicitada. En caso de negarla, el juez señalará los motivos de su negativa y los requisitos que deben cubrirse para la procedencia de ésta. La intervención puede aplicarse a comunicaciones y emisiones privadas, realizadas por cualquier medio de transmisión, conocido o por conocerse, o entre presentes, incluyendo la grabación de imágenes privadas	Artículo 39.- Una vez presentada la solicitud, el juez debe proporcionar acuse de recibo y emitir dentro de las veinticuatro horas contadas a partir de la solicitud, una resolución fundada y motivada en la que puede otorgar o negar la autorización solicitada. En caso de negarla, el juez señalará los motivos de su negativa y los requisitos que deben cubrirse para la procedencia de ésta. La intervención puede aplicarse a comunicaciones y emisiones privadas, realizadas por cualquier medio de transmisión, conocido o por conocerse, o entre presentes, incluyendo la grabación de imágenes privadas. **El Juez de control analizará la idoneidad, necesidad y proporcionalidad de la intervención y, en su caso, determinará sus características–modalidades, límites y en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración.** **No se podrán autorizar intervenciones o el empleo de tecnologías o métodos de colaboración que constituyan medidas de vigilancia masiva o indiscriminada, comprometan de manera masiva la seguridad e integridad de los sistemas de comunicación**

	o que no permitan al Juez hacer las verificaciones a las que se refiere el artículo 41.
Artículo 51.- Además de la información que satisfaga los criterios establecidos en la legislación general aplicable, es información reservada por motivos de Seguridad Nacional: I. Aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen, o II. Aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza.	Artículo 51.- ~~**Además de la información que satisfaga los criterios establecidos en la legislación general aplicable, es información reservada por motivos de Seguridad Nacional:**~~ ~~**I. Aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen, o**~~ ~~**II. Aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza.**~~ **Lo señalado en los artículos 37, 42, 45 y 48 de esta Ley no deberá obstaculizar el ejercicio de las facultades de supervisión, fiscalización o investigación, llevadas a cabo por las autoridades competentes, respecto de las responsabilidades administrativas o penales en que incurran los funcionarios públicos. Tampoco obstaculizará el derecho de acceso a la información en los términos establecidos por la Ley Federal de Transparencia y Acceso a la Información Pública.**
Artículo 52.- La publicación de información no reservada, generada o custodiada por el Centro, se realizará invariablemente con apego al principio de la información confidencial gubernamental.	Artículo 52.- ~~**La publicación de información no reservada, generada o custodiada por el Centro, se realizará invariablemente con apego al principio de la información confidencial gubernamental.**~~ **Tras la conclusión de la intervención, el Órgano jurisdiccional ordenará que las personas objeto de la intervención sean notificadas de conformidad con lo que señala la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.**

	Cuando sea necesario para evitar un riesgo inminente a la seguridad nacional o a la vida o integridad de una persona, la notificación podrá prorrogarse por un plazo no mayor a seis meses posterior a la conclusión de la intervención, previa autorización del juez que autorizó la misma.
Artículo 54.- La persona que por algún motivo participe o tenga conocimiento de productos, fuentes, métodos, medidas u operaciones de inteligencia, registros o información derivados de las acciones previstas en la presente Ley, debe abstenerse de difundirlo por cualquier medio y adoptar las medidas necesarias para evitar que lleguen a tener publicidad.	Artículo 54.- La persona que por algún motivo participe o tenga conocimiento de productos, fuentes, métodos, medidas u operaciones de inteligencia, registros o información derivados de las acciones previstas en la presente Ley, debe abstenerse de difundirlo por cualquier medio y adoptar las medidas necesarias para evitar que lleguen a tener publicidad**, sin perjuicio de las facultades de supervisión, fiscalización o investigación, llevadas a cabo por las autoridades competentes, respecto de las responsabilidades administrativas o penales en que incurran los funcionarios públicos, ni de lo establecido por la Ley Federal de Transparencia y Acceso a la Información Pública.**
Artículo 63.- Los datos personales de los sujetos que proporcionen información, serán confidenciales.	Artículo 63.- Los datos personales de los sujetos que proporcionen información, serán confidenciales. **El Centro colaborará con la autoridad en materia de protección de datos personales en el ejercicio de las facultades de supervisión y verificación a las que se refiere la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.**

D. Ley Federal contra la Delincuencia Organizada

LEY FEDERAL CONTRA LA DELINCUENCIA ORGANIZADA VIGENTE	PROPUESTA DE REFORMA
Artículo 7o.- Los procedimientos que se sigan	**Artículo 7o.-** Los procedimientos que se sigan

por delincuencia organizada se desahogarán de conformidad con lo previsto en el Código Nacional de Procedimientos Penales en lo que no se oponga a lo previsto en esta Ley. Son aplicables supletoriamente a esta Ley, las disposiciones del Código Penal Federal, las de la legislación que establezca las normas sobre ejecución de penas, así como las comprendidas en leyes especiales.	por delincuencia organizada se desahogarán de conformidad con lo previsto en el Código Nacional de Procedimientos Penales en lo que no se oponga a lo previsto en esta Ley**, así como en lo señalado por la Ley General de Protección de Datos en Posesión de Sujetos Obligados**. Son aplicables supletoriamente a esta Ley, las disposiciones del Código Penal Federal, las de la legislación que establezca las normas sobre ejecución de penas, así como las comprendidas en leyes especiales.
Artículo 11 Bis 1.- Para la investigación de los delitos a que se refiere esta Ley, el agente del Ministerio Público de la Federación podrá emplear además de los instrumentos establecidos en las disposiciones aplicables para la obtención de información y, en su caso, medios de prueba, así como las técnicas de investigación previstas en el Código Nacional de Procedimientos Penales, las siguientes: **I.** Recabar información en lugares públicos, mediante la utilización de medios e instrumentos y cualquier herramienta que resulten necesarias para la generación de inteligencia; **II.** Utilización de cuentas bancarias, financieras o de naturaleza equivalente; **III.** Vigilancia electrónica; **IV.** Seguimiento de personas; **V.** Colaboración de informantes, y **VI.** Usuarios simulados. Para el empleo de las técnicas previstas en las fracciones I y III de este artículo siempre que con su aplicación resulten afectadas comunicaciones privadas, se requerirá de una autorización judicial previa de intervención de comunicaciones privadas. El Fiscal General de la República emitirá los protocolos para el uso de las técnicas de investigación previstas en este artículo.	**Artículo 11 Bis 1.-** Para la investigación de los delitos a que se refiere esta Ley, el agente del Ministerio Público de la Federación podrá emplear además de los instrumentos establecidos en las disposiciones aplicables para la obtención de información y, en su caso, medios de prueba, así como las técnicas de investigación previstas en el Código Nacional de Procedimientos Penales, las siguientes: **I.** Recabar información en lugares públicos, mediante la utilización de medios e instrumentos y cualquier herramienta que resulten **idóneas,** necesarias **y proporcionales** para la generación de inteligencia; **II.** Utilización de cuentas bancarias, financieras o de naturaleza equivalente; **III.** Vigilancia electrónica; **IV.** Seguimiento de personas; **V.** Colaboración de informantes, y **VI.** Usuarios simulados. Para el empleo de las técnicas previstas en las fracciones I y III de este artículo siempre que con su aplicación resulten afectadas comunicaciones privadas, **incluyendo datos de tráfico de comunicaciones y geolocalización de dispositivos** se requerirá de una autorización judicial **federal** previa ~~**de intervención de comunicaciones privadas**~~. **No se podrán autorizar medidas de recolección de información en lugares públicos, de vigilancia electrónica o el empleo de tecnologías o métodos de colaboración que**

	constituyan medidas de vigilancia masiva o indiscriminada, comprometan de manera masiva la seguridad e integridad de los sistemas de comunicación o que no permitan al Juez ejercer las facultades de verificación del cumplimiento de sus resoluciones. El Fiscal General de la República emitirá los protocolos para el uso de las técnicas de investigación previstas en este artículo.
Artículo 13.- A los registros de la investigación por los delitos a que se refiere esta Ley, exclusivamente deberán tener acceso el imputado y su defensor que haya aceptado el cargo, en términos de lo previsto por los artículos 218, 219 y 220 del Código Nacional de Procedimientos Penales únicamente con relación a los hechos imputados en su contra, por lo que el agente del Ministerio Público de la Federación y sus auxiliares guardarán la mayor reserva respecto de ellas. Para efectos de seguridad de las víctimas o los actores procesales, si el órgano jurisdiccional lo determina de oficio o a petición de parte, las audiencias celebradas en el procedimiento penal por delitos de delincuencia organizada, se desarrollarán a puerta cerrada.	**Artículo 13.-** A los registros de la investigación por los delitos a que se refiere esta Ley, exclusivamente deberán tener acceso el imputado y su defensor que haya aceptado el cargo, en términos de lo previsto por los artículos 218, 219 y 220 del Código Nacional de Procedimientos Penales únicamente con relación a los hechos imputados en su contra, por lo que el agente del Ministerio Público de la Federación y sus auxiliares guardarán la mayor reserva respecto de ellas. **Lo anterior no deberá obstaculizar el ejercicio de las facultades de supervisión, fiscalización o investigación, llevadas a cabo por las autoridades competentes, respecto de las responsabilidades administrativas o penales en que incurran los funcionarios públicos. Tampoco obstaculizará el derecho de acceso a la información en los términos establecidos por la Ley Federal de Transparencia y Acceso a la Información Pública.** Para efectos de seguridad de las víctimas o los actores procesales, si el órgano jurisdiccional lo determina de oficio o a petición de parte, las audiencias celebradas en el procedimiento penal por delitos de delincuencia organizada, se desarrollarán a puerta cerrada.
Artículo 16.- Cuando en la investigación el Ministerio Público de la Federación considere necesaria la intervención de comunicaciones privadas el Fiscal General de la República o los servidores públicos en quienes se delegue la facultad podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.	**Artículo 16.-** Cuando en la investigación el Ministerio Público de la Federación considere necesaria la intervención de comunicaciones privadas el Fiscal General de la República o los servidores públicos en quienes se delegue la facultad podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.

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. La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público de la Federación, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público de la Federación. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.	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. La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público de la Federación, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. **También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos.** Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público de la Federación. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.
Artículo 17.- La solicitud de intervención de comunicaciones privadas deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos y, en su caso, la denominación de la empresa concesionaria del servicio de telecomunicaciones a través del cual se realiza la	**Artículo 17.-** La solicitud de intervención de comunicaciones privadas deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos y, en su caso, la denominación de la empresa concesionaria del servicio de telecomunicaciones **o la empresa prestadora de**

comunicación objeto de la intervención. El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público de la Federación acredite nuevos elementos que así lo justifiquen.	**servicios, aplicaciones o contenidos en Internet** a través del cual se realiza la comunicación objeto de la intervención**, así como la tecnología empleada para llevar a cabo la intervención.** El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público de la Federación acredite nuevos elementos que así lo justifiquen.
Artículo 18.- En la autorización, el Juez de control determinará las características de la intervención, sus modalidades, límites y, en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración. Podrán ser objeto de intervención 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. En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su Defensor. El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total. Cuando de la intervención de comunicaciones privadas se advierta la necesidad de ampliarla a otros sujetos o lugares, el Ministerio Público de la Federación competente presentará al propio Juez de control la solicitud respectiva.	**Artículo 18.-** En la autorización, el Juez de control **analizará la idoneidad, necesidad y proporcionalidad de la intervención y** determinará l**as sus** características~~ de la intervención, sus~~ modalidades, límites y, en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración. Podrán ser objeto de intervención 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. En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su Defensor. El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total. **No se podrán autorizar intervenciones o el empleo de tecnologías o métodos de colaboración que constituyan medidas de vigilancia masiva o indiscriminada, comprometan de manera masiva la seguridad e integridad de los sistemas de comunicación o que no permitan al Juez hacer las verificaciones a las que se refiere el párrafo anterior.** Cuando de la intervención de comunicaciones privadas se advierta la necesidad de ampliarla a otros sujetos o lugares, el Ministerio Público de la

	Federación competente presentará al propio Juez de control la solicitud respectiva.
Artículo 20.- Las intervenciones de comunicación deberán ser registradas por cualquier medio que no altere la fidelidad, autenticidad y contenido de las mismas, por quienes las ejecuten, a efecto de que aquélla pueda ser ofrecida como medio de prueba en los términos que señala el Código Nacional de Procedimientos Penales. El registro contendrá las fechas de inicio y término de la intervención, un inventario pormenorizado de los documentos, objetos y los medios para la reproducción de sonidos o imágenes captadas durante la misma, cuando no se ponga en riesgo a la investigación o a la persona, la identificación de quienes hayan participado en los actos de investigación, así como los demás datos que se consideren relevantes para la investigación. El registro original y el duplicado, así como los documentos que los integran, se numerarán progresivamente y contendrán los datos necesarios para su identificación.	**Artículo 20.-** Las intervenciones de comunicación deberán ser registradas por cualquier medio que no altere la fidelidad, autenticidad y contenido de las mismas, por quienes las ejecuten, a efecto de que aquélla pueda ser ofrecida como medio de prueba en los términos que señala el Código Nacional de Procedimientos Penales. El registro contendrá las fechas de inicio y término de la intervención, un inventario pormenorizado de los documentos, objetos y los medios para la reproducción de sonidos o imágenes captadas durante la misma, cuando no se ponga en riesgo a la investigación o a la persona, la identificación de quienes hayan participado en los actos de investigación, **la tecnología o método de colaboración empleado,** así como los demás datos que se consideren relevantes para la investigación. El registro original y el duplicado, así como los documentos que los integran, se numerarán progresivamente y contendrán los datos necesarios para su identificación.
Artículo 24.- El Órgano jurisdiccional ordenará la destrucción de aquellos registros de intervención de comunicaciones privadas que no se relacionen con los delitos investigados o con otros delitos que hayan ameritado la apertura de una investigación diversa, salvo que la defensa solicite que sean preservados por considerarlos útiles para su labor. Asimismo, ordenará la destrucción de los registros de intervenciones no autorizadas o cuando éstos rebasen los términos de la autorización judicial respectiva. Los registros serán destruidos cuando se decrete el archivo definitivo, el sobreseimiento o la absolución del imputado. Cuando el agente del Ministerio Público de la Federación decida archivar temporalmente la investigación, los registros podrán ser conservados hasta que el delito prescriba.	Artículo 24.- El Órgano jurisdiccional ordenará la destrucción de ~~**aquellos registros de intervención de comunicaciones privadas**~~ **la información obtenida mediante la intervención o extracción** que no se relacione~~**n**~~ con los delitos investigados o con otros delitos que hayan ameritado la apertura de una investigación diversa, salvo que la **persona objeto de la intervención** ~~**defensa**~~**, previa notificación de la misma,** solicite que sean preservados por considerarlos útiles para su**s intereses** ~~**labor**~~. Asimismo, ordenará la destrucción de ~~**los registros de intervenciones**~~ **la información obtenida mediante la intervención** no autorizada~~**s**~~ o cuando ~~**éstos**~~ rebase~~**n**~~ los términos de la autorización judicial respectiva**, previa notificación de la intervención a la persona objeto de la misma**, **en términos de lo que indica la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.** ~~**Los registros**~~ **La información obtenida mediante la intervención** será~~**n**~~ destruid~~**aos**~~ cuando se decrete el archivo definitivo, el sobreseimiento o la absolución del imputado **previa notificación de la intervención a la persona objeto de la misma**. Cuando el

	Ministerio Público decida archivar temporalmente la investigación, ~~**los registros**~~ **la información obtenida mediante la intervención** podrá~~**n**~~ ser conservad~~**aos**~~ hasta que el delito prescriba. **De manera previa a la destrucción de la información obtenida mediante la intervención, el Órgano jurisdiccional ordenará que las personas objeto de la intervención sean notificadas de conformidad con lo que señala la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.** **Cuando sea necesario para no poner en riesgo la investigación o a persona alguna, la notificación podrá prorrogarse por un plazo no mayor a seis meses después de la conclusión de la intervención.**
Artículo 26.- Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con las disposiciones aplicables. Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas. El incumplimiento a este mandato será sancionado conforme a las disposiciones penales aplicables.	Artículo 26.- Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con ~~**las disposiciones aplicables**~~ **lo ordenado por el Juez de Control competente**. ~~**Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas.**~~ El incumplimiento a este mandato será sancionado conforme a las disposiciones penales aplicables.
Artículo 28.- Quienes participen en alguna intervención de comunicaciones privadas deberán guardar reserva sobre el contenido de las mismas. Los servidores públicos de la unidad especializada prevista en el artículo 8o. de esta Ley, así como cualquier otro servidor público o los servidores públicos del Poder Judicial Federal, que participen en algún proceso de los delitos a que se refiere esta Ley, que revelen, divulguen o utilicen en forma indebida o en perjuicio de otro la información o imágenes obtenidas en el curso de una intervención de comunicaciones privadas, autorizada o no, serán sancionados con prisión de seis a doce años, de quinientos a mil días multa, así como con la destitución e inhabilitación para	Artículo 28.- Quienes participen en alguna intervención de comunicaciones privadas deberán guardar reserva sobre el contenido de las mismas. Los servidores públicos de la unidad especializada prevista en el artículo 8o. de esta Ley, así como cualquier otro servidor público o los servidores públicos del Poder Judicial Federal, que participen en algún proceso de los delitos a que se refiere esta Ley, que revelen, divulguen o utilicen en forma indebida o en perjuicio de otro la información o imágenes obtenidas en el curso de una intervención de comunicaciones privadas, autorizada o no, serán sancionados con prisión de seis a doce años, de quinientos a mil días multa, así como con la destitución e inhabilitación para

desempeñar otro empleo, cargo o comisión públicos, por el mismo plazo que la pena de prisión impuesta. La misma pena se impondrá a quienes con motivo de su empleo, cargo o comisión público tengan conocimiento de la existencia de una solicitud o autorización de intervención de comunicaciones privadas y revelen su existencia o contenido.	desempeñar otro empleo, cargo o comisión públicos, por el mismo plazo que la pena de prisión impuesta. La misma pena se impondrá a quienes con motivo de su empleo, cargo o comisión público tengan conocimiento de la existencia de una solicitud o autorización de intervención de comunicaciones privadas y revelen su existencia o contenido. **Lo señalado en este artículo no deberá obstaculizar el ejercicio de las facultades de supervisión, fiscalización o investigación, llevadas a cabo por las autoridades competentes, respecto de las responsabilidades administrativas o penales en que incurran los funcionarios públicos. Tampoco obstaculizará el derecho de acceso a la información en los términos establecidos por la Ley Federal de Transparencia y Acceso a la Información Pública.**

E. Código Militar de Procedimientos Penales

CÓDIGO MILITAR DE PROCEDIMIENTOS PENALES VIGENTE	PROPUESTA DE REFORMA
Artículo 287. Intervención de las comunicaciones privadas respecto de hechos que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia de la justicia castrense Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Fiscalía General de Justicia Militar o el servidor público facultado, en quien delegue ésta, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma. 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	**Artículo 287. Intervención de las comunicaciones privadas respecto de hechos que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia de la justicia castrense** Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Fiscalía General de Justicia Militar o el servidor público facultado, en quien delegue ésta, podrán solicitar al Juez federal de control **civil** competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma. 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. También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos. La solicitud deberá ser resuelta por el Juez de control de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.	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. También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos. La solicitud deberá ser resuelta por el Juez de control de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.
Artículo 288. Requisitos de la solicitud La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención. El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse	**Artículo 288. Requisitos de la solicitud** La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones **o la empresa prestadora de servicios, aplicaciones o contenidos en Internet** a través del cual se realiza la comunicación objeto de la intervención**, así como la tecnología empleada para llevar a cabo la intervención.**

nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.	El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.
Artículo 289. Contenido de la resolución judicial que autoriza la intervención de las comunicaciones privadas respecto de hechos que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia de la justicia castrense En la autorización, el Juez de control determinará las características de la intervención, sus modalidades, límites y en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.	**Artículo 289. Contenido de la resolución judicial que autoriza la intervención de las comunicaciones privadas respecto de hechos que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia de la justicia castrense** En la autorización, el Juez de control **analizará la idoneidad, necesidad y proporcionalidad de la intervención y** determinará ~~**las**~~ **sus** características~~ **de la intervención, sus**~~ modalidades, límites y en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.
Artículo 290. Objeto de la intervención respecto de hechos que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia de la justicia castrense Podrán ser objeto de intervención 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. La intervención de comunicaciones privadas a que se refiere este capítulo, solo podrá autorizarse en la investigación de delitos de la competencia de los Órganos Jurisdiccionales Militares. El Juez de control podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.	**Artículo 290. Objeto de la intervención respecto de hechos que se investigan, probablemente cometidos por personal militar, en el ámbito de competencia de la justicia castrense** Podrán ser objeto de intervención 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. La intervención de comunicaciones privadas a que se refiere este capítulo, solo podrá autorizarse en la investigación de delitos de la competencia de los Órganos Jurisdiccionales Militares. El Juez de control podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total. **No se podrán autorizar intervenciones o el empleo de tecnologías o métodos de colaboración que comprometan de manera masiva la seguridad e integridad de los**

	sistemas de comunicación o que no permitan al Juez hacer las verificaciones a las que se refiere el párrafo anterior.
Artículo 294. Registro El registro a que se refiere el artículo anterior contendrá las fechas de inicio y término de la intervención, un inventario pormenorizado de los documentos, objetos y los medios para la reproducción de sonidos o imágenes captadas durante la misma, cuando no se ponga en riesgo a la investigación o a la persona, la identificación de quienes hayan participado en los actos de investigación, así como los demás datos que se consideren relevantes para la investigación. El registro original y el duplicado, así como los documentos que los integran, se numerarán progresivamente y contendrán los datos necesarios para su identificación.	**Artículo 294. Registro** El registro a que se refiere el artículo anterior contendrá las fechas de inicio y término de la intervención, un inventario pormenorizado de los documentos, objetos y los medios para la reproducción de sonidos o imágenes captadas durante la misma, cuando no se ponga en riesgo a la investigación o a la persona, la identificación de quienes hayan participado en los actos de investigación, **la tecnología o método de colaboración empleado,** así como los demás datos que se consideren relevantes para la investigación. El registro original y el duplicado, así como los documentos que los integran, se numerarán progresivamente y contendrán los datos necesarios para su identificación. **Tras la conclusión de la intervención, el Órgano jurisdiccional federal civil ordenará que las personas objeto de la intervención sean notificadas de conformidad con lo que señala la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.** **Cuando sea necesario para evitar un riesgo inminente a la seguridad nacional o a la vida o integridad de una persona, la notificación podrá prorrogarse por un plazo no mayor a seis meses posterior a la conclusión de la intervención, previa autorización del juez que autorizó la misma.**
Artículo 297. Colaboración con la autoridad Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con las disposiciones aplicables. Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por el Órgano jurisdiccional militar para operar una orden de intervención de comunicaciones privadas. El incumplimiento a este mandato será sancionado conforme a las disposiciones penales	**Artículo 297. Colaboración con la autoridad** Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con **~~las disposiciones aplicables~~ lo ordenado por el Juez de Control federal civil**. **~~Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por el Órgano jurisdiccional militar para operar una orden de intervención de comunicaciones privadas.~~** El incumplimiento a este mandato será

aplicables.	sancionado conforme a las disposiciones penales aplicables.
Artículo 298. Deber de secrecía Quienes participen en alguna intervención de comunicaciones privadas deberán observar el deber de secrecía sobre el contenido de las mismas.	Artículo 298. Deber de secrecía ~~**Quienes participen**~~ **Los funcionarios públicos que tengan conocimiento de información obtenida** en alguna intervención de comunicaciones privadas deberán observar el deber de secrecía sobre el contenido de las mismas. **Lo anterior no deberá obstaculizar el ejercicio de las facultades de supervisión, fiscalización o investigación, llevadas a cabo por las autoridades competentes, respecto de las responsabilidades administrativas o penales en que incurran los funcionarios públicos a los que se refiere el párrafo anterior.**

F. Ley Federal de Telecomunicaciones y Radiodifusión

LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN	PROPUESTA DE REFORMA
Artículo 189. Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes. Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.	**Artículo 189.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que ~~**establezcan las leyes**~~ **establece el Código Nacional de Procedimientos Penales, la Ley de Seguridad Nacional, la Ley de la Guardia Nacional y el Código Militar de Procedimientos Penales, previa autorización judicial federal.** Los titulares de las instancias de seguridad y procuración de justicia **competentes** designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.
Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán: I. Colaborar con las instancias de seguridad,	**Artículo 190.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán: I. Colaborar con las ~~**instancias de seguridad,**~~

procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes. Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable. El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna; II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos: a) Nombre, denominación o razón social y domicilio del suscriptor; b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados); c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago; d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia; e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio; f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor; g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que	~~**procuración y administración de justicia**~~ **autoridades competentes en términos del artículo anterior**, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes. Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable. El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, **a las empresas concesionarias, autorizadas, a los proveedores de servicios, aplicaciones y contenidos, así como a las organizaciones de la sociedad civil interesadas**, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna; II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos: a) Nombre, denominación o razón social y domicilio del suscriptor; b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados); c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago; d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia; e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio; f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de

se haya producido la comunicación. Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud. La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo. Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control. Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; III. Entregar los datos conservados a las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables. Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten. Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo	fabricación del equipo y del suscriptor; g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación. Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior**, respecto de las líneas que sean especificadas en el requerimiento, hasta por un tiempo máximo de noventa días a partir del requerimiento, sujeto a una sola prórroga por 90 días adicionales.** ~~durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos~~. ~~Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.~~ La solicitud y entrega ~~**en tiempo real**~~ de los datos referidos en este inciso, se realizará mediante l**os mecanismos establecidos en las Leyes y en los Lineamientos a los que se refiere la fracción I de este artículo**. ~~**que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.**~~ Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control. **Los concesionarios de telecomunicaciones y, en su caso, los autorizados mantendrán medidas de registro y control de los requerimientos en los que se incluirá el nombre los empleados encargados de la tramitación de los requerimientos y otros datos que señale el Instituto en los Lineamientos.**

máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente;	Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, **incluyendo respecto del derecho de acceso a los usuarios a los datos conservados en virtud de esta fracción**; III. Entregar, **previa autorización judicial federal**, los datos conservados a las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables. **Excepcionalmente podrán entregarse datos conservados o el acceso a la geolocalización, en tiempo real, de equipos de comunicación móvil, sin previa autorización judicial en los casos establecidos explícitamente en las leyes correspondientes. Transcurrido el plazo para la ratificación de la medida por parte del Juez de Control, los concesionarios, y en su caso, los autorizados darán aviso a la autoridad judicial federal competente.** Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten. Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente; **Los concesionarios de telecomunicaciones y, en su caso, los autorizados, así como los proveedores de aplicaciones, contenidos y servicios en Internet deberán entregar al Instituto, en los meses de enero, abril, julio y octubre de cada año, un informe trimestral electrónico a través del mecanismo que para tales efectos establezca el Instituto, relativo a los requerimientos de colaboración para la intervención de comunicaciones privadas, geolocalización ,en tiempo real, de equipos de comunicación móvil, así como la conservación y acceso a datos conservados.**

	Dicho informe deberá contener y observar lo siguiente: **I. El número total y por autoridad, de requerimientos de colaboración para la intervención de comunicaciones privadas, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando las recibidas, entregadas y no entregadas mensualmente, así como las que fueron recibidas previa autorización judicial y las que se realizaron en los casos de excepción, de las cuales deberá indicarse el número de requerimientos excepcionales cuya ratificación por parte del Juez de control fue notificada, utilizando el formato que defina el Instituto.** **II. El número total y por autoridad de avisos de notificación de medidas excepcionales en los términos en que señala el presente artículo.** **La información estadística contenida en los informes trimestrales será publicada en el portal de Internet del Instituto en términos de lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables.** **Los concesionarios y autorizados de telecomunicaciones y, en su caso, los proveedores de aplicaciones, contenidos y servicios en Internet, colaborarán con la autoridad judicial federal para la notificación de personas objeto de medidas de intervención de comunicaciones privadas, geolocalización, en tiempo real, de equipos de comunicación móvil y el acceso a datos conservados, en los términos que señala la autoridad judicial y las leyes correspondientes.** **En caso de que los sistemas de conservación de datos hayan sido vulnerados y los Datos Personales de los usuarios finales se encuentren comprometidos, los Concesionarios y Autorizados deberán notificar inmediatamente al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y a los usuarios afectados e indicará las medidas que el usuario podrá tomar para disminuir o contrarrestar cualquier afectación derivada de**

	esta vulneración.

G. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS	PROPUESTA DE REFORMA
Capítulo II De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia **Artículo 80**. La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de las sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto. Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente Capítulo.	Capítulo II ~~**De las Bases de Datos en Posesión de**~~ **Del tratamiento de datos personales por parte de Instancias de Seguridad, Procuración y Administración de Justicia** **Artículo 80.** La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de las sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto. Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente Capítulo.
Artículo 81. En el tratamiento de datos personales así como en el uso de las bases de datos para su almacenamiento, que realicen los sujetos obligados competentes de las instancias de seguridad, procuración y administración de justicia deberá cumplir con los principios establecidos en el Título Segundo de la presente Ley. Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.	Artículo 81. En el tratamiento de datos personales así como en el uso de las bases de datos para su almacenamiento, que realicen los sujetos obligados competentes de las instancias de seguridad, procuración y administración de justicia deberá cumplir con los principios establecidos en el Título Segundo de la presente Ley. Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.
Artículo 82. Los responsables de las bases de datos a que se refiere este Capítulo, deberán	Artículo 82. Los responsables de las bases de datos a que se refiere este Capítulo, deberán

establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. **Las tecnologías utilizadas para la obtención y tratamiento de datos personales a que se refiere este capítulo deberán contar con medidas que permitan la auditoría, trazabilidad y rendición de cuentas.**
Artículo 82 Bis. (NO EXISTE)	**Artículo 82 Bis.- Las medidas de vigilancia como la intervención de comunicaciones privadas, la extracción de información, la geolocalización en tiempo real de equipos de comunicación móvil y el acceso a datos conservados por concesionarios y autorizados para prestar servicios de telecomunicaciones o por proveedores de servicios, aplicaciones y contenidos en Internet solo podrá realizarse de conformidad con lo que establecen el Código Nacional de Procedimientos Penales, la Ley de Seguridad Nacional, la Ley de la Guardia Nacional, el Código Militar de Procedimientos Penales, la Ley Federal de Telecomunicaciones y Radiodifusión, así como en las disposiciones de este Capítulo.** **Salvo los casos excepcionales a los que se refiere el artículo 303 del Código Nacional de Procedimientos Penales, sujetos a ratificación inmediata por parte de la autoridad judicial federal, las medidas señaladas en el párrafo anterior solo podrán ser llevadas a cabo previa autorización del Juez de Control federal competente.** **Las solicitudes de autorización judicial deberán precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números, cuentas o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones o la empresa prestadora de servicios, aplicaciones o contenidos en Internet a través del cual se realiza la comunicación objeto de la medida, así como la tecnología empleada para llevar a cabo la misma.**

	El Juez de control analizará la idoneidad, necesidad y proporcionalidad de las medidas y, en su caso, determinará sus características modalidades, límites y en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración. **No se podrán autorizar medidas de vigilancia indiscriminada o masiva o el empleo de tecnologías o métodos de colaboración que comprometan de manera masiva la seguridad e integridad de los sistemas de comunicación o que no permitan al Juez verificar que las medidas sean realizadas en los términos autorizados.**
Artículo 82 Ter. (NO EXISTE)	**Artículo 82 Ter.- Las autoridades facultadas por las leyes a las que hace referencia el primer párrafo del artículo anterior deberán establecer mecanismos de control de las medidas de vigilancia, que incluyan, como mínimo el registro de:** **I. Tipo de medida de vigilancia empleada;** **II. Fundamentación y motivación;** **III. Fecha de inicio y término de la medida;** **IV. Número y nombre de las personas objeto de la medida;** **V. Identificación de los lugares, líneas, números, aparatos o cuentas objeto de la medida;** **VI. En su caso, denominación de las concesionarias y autorizadas, así como de los prestadores de servicios, aplicaciones y contenidos en Internet que hayan colaborado para llevar a cabo la medida;** **VII. En su caso, tecnología o método de colaboración empleado;** **VIII. Nombre de los funcionarios públicos que participaron en la medida;** **IX. Datos de identificación del expediente, carpeta de investigación o asunto relacionado con la medida;** **X. Datos de identificación de la autorización judicial correspondiente; y** **XI. El registro de las comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, datos de localización, 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 que hayan sido obtenidos mediante la medida de vigilancia. **XII. Cualquier otro dato requerido por las leyes correspondientes o por los Lineamientos que establezcan las autoridades competentes.** **Únicamente será reservada la información que cumpla con los requisitos que establece la Ley General de Transparencia y Acceso a la Información Pública.** **Únicamente podrá ser destruida la información a la que se refiere el inciso XI del presente artículo, cuando así lo determine la autoridad judicial federal competente, previa notificación de dicha información a la persona afectada en los términos de lo que señala el artículo siguiente.** **Los deberes de secrecía no deberán obstaculizar el ejercicio de las facultades de supervisión, fiscalización o investigación, llevadas a cabo por las autoridades competentes, incluyendo al Instituto, respecto de las responsabilidades administrativas o penales en que incurran los funcionarios públicos en relación a las medidas de vigilancia a las que se refiere el presente Capítulo.** **Tampoco obstaculizarán el derecho de acceso a la información en los términos establecidos por la Ley General de Transparencia y Acceso a la Información Pública.**
Artículo 82 Quáter.	**Artículo 82 Quáter.- Las personas objeto de las medidas de vigilancia a las que se refiere el presente Capítulo tienen derecho a que, una vez concluidas las medidas de vigilancia, sean notificadas, por el Juez de control competente, de haber sido sujetas a dichas medidas y a conocer la información obtenida.** **La notificación podrá ser prorrogada por única vez, mediante solicitud de la autoridad competente al Juez de Control que autorizó la medida, cuando esté en peligro la integridad física o la vida de una persona o se encuentre**

	en riesgo el objeto del delito o la seguridad nacional. **La prórroga no podrá exceder del plazo de seis meses posteriores a la conclusión de la medida.** **Las autoridades competentes ordenarán la colaboración de los concesionarios y autorizados de telecomunicaciones, así como los proveedores de aplicaciones, contenidos y servicios en Internet para efectuar la notificación ordenada por el Juez de control.**
	Artículo 82 Quintus.- El Instituto realizará procedimientos de vigilancia y verificación oficiosa de manera aleatoria para verificar el cumplimiento de las disposiciones del presente Capítulo. **El Instituto elaborará un Informe Anual sobre la fiscalización de medidas de vigilancia en el que presentará sus hallazgos y formulará recomendaciones a las autoridades facultadas. El informe será público, por lo que no deberá revelar información que válidamente deba reservarse, de conformidad con lo que señala la Ley General de Transparencia y Acceso a la Información Pública.**
Artículo 89. Además de las facultades que le son conferidas en la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y demás normatividad que le resulte aplicable, el Instituto tendrá las siguientes atribuciones: (...) XXXVII. Las demás que le confiera la presente Ley y demás ordenamientos aplicables.	**Artículo 89.** Además de las facultades que le son conferidas en la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y demás normatividad que le resulte aplicable, el Instituto tendrá las siguientes atribuciones: (...) **XXXVII. Vigilar y verificar el cumplimiento de las disposiciones relacionadas con medidas de vigilancia a las que se refiere el Capítulo II del Título Sexto de la presente Ley, incluyendo realización de los procedimientos de verificación y la emisión del Informe Anual al que se refiere el artículo 82 Quintus de esta Ley.** **XXXVIII.** Las demás que le confiera la presente Ley y demás ordenamientos aplicables.
Artículo 147. La verificación podrá iniciarse: I. De oficio cuando el Instituto o los Organismos garantes cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes, o	**Artículo 147**. La verificación podrá iniciarse: I. De oficio cuando el Instituto o los Organismos garantes cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes **o de manera aleatoria**

II. Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable, o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia. El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma. (...)	**en cumplimiento de lo que señala el artículo 82 Quintus**, o II. Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable, o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia. El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma **o el Titular tenga conocimiento de los mismos**. (...)
Artículo 149. La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los Organismos garantes, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas. Para la verificación en instancias de seguridad nacional y seguridad pública, se requerirá en la resolución, la aprobación del Pleno del Instituto, por mayoría calificada de sus Comisionados, o de los integrantes de los Organismos garantes de las Entidades Federativas, según corresponda; así como de una fundamentación y motivación reforzada de la causa del procedimiento, debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines establecidos en el artículo 150. El procedimiento de verificación deberá tener una duración máxima de cincuenta días. El Instituto o los organismos garantes podrán ordenar medidas cautelares, si del desahogo de la verificación advierten un daño inminente o irreparable en materia de protección de datos personales, siempre y cuando no impidan el cumplimiento de las funciones ni el aseguramiento de bases de datos de los sujetos obligados.	**Artículo 149.** La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los Organismos garantes, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas. Para la verificación en instancias de seguridad nacional y seguridad pública, se requerirá en la resolución, la aprobación del Pleno del Instituto, por mayoría calificada de sus Comisionados, o de los integrantes de los Organismos garantes de las Entidades Federativas, según corresponda; así como de una fundamentación y motivación reforzada de la causa del procedimiento, debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines establecidos en ~~**el**~~ **los** artículo**s 82 Quintus y** 150. El procedimiento de verificación deberá tener una duración máxima de cincuenta días. **Excepto cuando, de manera motivada, el Instituto considere necesario prorrogar el plazo por tiempo indefinido cuando determine que el sujeto obligado no ha colaborado de manera efectiva con el procedimiento.** El Instituto o los organismos garantes podrán ordenar medidas cautelares, si del desahogo de la verificación advierten un daño inminente o irreparable en materia de protección de datos

Estas medidas sólo podrán tener una finalidad correctiva y será temporal hasta entonces los sujetos obligados lleven a cabo las recomendaciones hechas por el Instituto o los Organismos garantes según corresponda.	personales, siempre y cuando no impidan el cumplimiento de las funciones ni el aseguramiento de bases de datos de los sujetos obligados. Estas medidas sólo podrán tener una finalidad correctiva y será temporal hasta entonces los sujetos obligados lleven a cabo las recomendaciones hechas por el Instituto o los Organismos garantes según corresponda.

H. Ley General del Sistema Nacional de Seguridad Pública

LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA	PROPUESTA DE REFORMA
Artículo 110.- (...) Se clasifica como reservada la información contenida en todas y cada una de las Bases de Datos del Sistema Nacional de Información, así como los Registros Nacionales y la información contenida en ellos, en materia de detenciones, información criminal, personal de seguridad pública, personal y equipo de los servicios de seguridad privada, armamento y equipo, vehículos, huellas dactilares, teléfonos celulares, medidas cautelares, soluciones alternas y formas de terminación anticipada, sentenciados y las demás necesarias para la operación del Sistema, cuya consulta es exclusiva de las instituciones de Seguridad Pública que estén facultadas en cada caso, a través de los servidores públicos que cada institución designe, por lo que el público no tendrá acceso a la información que en ellos se contenga.	**Artículo 110.-** (...) Se clasifica como reservada la información **que cumpla con los requisitos establecidos en el Título Sexto de la Ley General de Transparencia y Acceso a la Información Pública** contenida en todas y cada una de las Bases de Datos del Sistema Nacional de Información, así como los Registros Nacionales y la información contenida en ellos, en materia de detenciones, información criminal, personal de seguridad pública, personal y equipo de los servicios de seguridad privada, armamento y equipo, vehículos, huellas dactilares, teléfonos celulares, medidas cautelares, soluciones alternas y formas de terminación anticipada, sentenciados y las demás necesarias para la operación del Sistema, ~~**cuya consulta es exclusiva de las instituciones de Seguridad Pública que estén facultadas en cada caso, a través de los servidores públicos que cada institución designe, por lo que el público no tendrá acceso a la información que en ellos se contenga.**~~
Artículo 124.- Además de cumplir con las disposiciones contenidas en otras leyes, las autoridades competentes de la Federación, las entidades federativas y los Municipios manifestarán y mantendrán actualizado el Registro Nacional de Armamento y Equipo. Dicha Base de Datos deberá contener: I. La información de los vehículos que tuvieran asignados, anotándose el número de matrícula, las placas de circulación, la marca, modelo, tipo, número de serie y motor para el registro del	**Artículo 124.-** Además de cumplir con las disposiciones contenidas en otras leyes, las autoridades competentes de la Federación, las entidades federativas y los Municipios manifestarán y mantendrán actualizado el Registro Nacional de Armamento y Equipo. Dicha Base de Datos deberá contener: I. La información de los vehículos que tuvieran asignados, anotándose el número de matrícula, las placas de circulación, la marca, modelo, tipo, número de serie y motor para el registro del

vehículo, y II. La información de las armas y municiones que les hayan sido autorizadas por las dependencias competentes, aportando el número de registro, la marca, modelo, calibre, matrícula, huella balística y demás elementos de identificación que exijan la ley de la materia y su reglamento.	vehículo, y II. La información de las armas y municiones que les hayan sido autorizadas por las dependencias competentes, aportando el número de registro, la marca, modelo, calibre, matrícula, huella balística y demás elementos de identificación que exijan la ley de la materia y su reglamento. **III. La información de los equipos y sistemas tecnológicos para la intervención de comunicaciones privadas o la geolocalización de equipos de comunicación móvil que sean utilizados por las autoridades competentes, aportando los elementos de información que exijan las leyes de la materia y su reglamento.**
Artículo 125.- (...)	**Artículo 125.- (...)** **Las instituciones de Seguridad Pública competentes, mantendrán un registro de los elementos autorizados para la operación de los equipos y sistemas tecnológicos para la intervención de comunicaciones privadas o la geolocalización en tiempo real de equipos comunicación móvil.** **Igualmente, mantendrán un registro detallado de uso de los equipos y sistemas tecnológicos para la intervención de comunicaciones privadas o la geolocalización en tiempo real de equipos de comunicación móvil. Deberán implementarse medidas efectivas para garantizar la detección del uso no registrado de los equipos y sistemas tecnológicos o para prevenir la alteración de los registros.**
Artículo 127.- El incumplimiento de las disposiciones de esta sección, dará lugar a que la portación o posesión de armas se considere ilegal y sea sancionada en los términos de las normas aplicables.	**Artículo 127.-** El incumplimiento de las disposiciones de esta sección, dará lugar a que la portación**, ~~o~~** posesión de armas **o utilización de equipos y sistemas tecnológicos para la intervención de comunicaciones privadas o la geolocalización en tiempo real de equipos de comunicación móvil** se considere ilegal y sea sancionada en los términos de las normas aplicables.
(No existe)	**TÍTULO DÉCIMO TERCERO** **DE LA COMERCIALIZACIÓN DE EQUIPOS Y SISTEMAS TECNOLÓGICOS PARA LA INTERVENCIÓN DE COMUNICACIONES PRIVADAS Y LA GEOLOCALIZACIÓN EN TIEMPO REAL DE EQUIPOS DE COMUNICACIÓN MÓVIL**

	Artículo 153.- Además de cumplir con otras disposiciones aplicables, los particulares que comercialicen equipos o sistemas tecnológicos para la intervención de comunicaciones privadas o la geolocalización de equipos de comunicación móvil, deberán obtener autorización previa de la Secretaría. **Artículo 154.- La solicitud deberá contener por lo menos lo siguiente:** **I. Nombre o razón social de la persona autorizada.** **II. Domicilio y teléfono.** **III. Nombre comercial y descripción general de los equipos o sistemas tecnológicos respecto de los cuales se solicita autorización para comercializar.** **IV. Nombre o razón social de las personas fabricantes, desarrolladoras o prestadoras finales de los servicios, equipos o sistemas tecnológicos a comercializar.** **V. En su caso, el país de origen de la personas a las que se refiere el párrafo anterior.** **VI. Carta de ausencia de impedimentos legales o contractuales para colaborar con las autoridades competentes para investigar conductas relacionadas con el uso ilegal de los servicios, equipos o sistemas tecnológicos.** **VII. La información adicional que determine la Secretaría.** **Artículo 155.- La Secretaría no autorizará la comercialización de servicios, equipos o sistemas tecnológicos para la intervención de comunicaciones privadas o geolocalización en tiempo real de equipos de comunicación móvil cuando:** **I. Los servicios, equipos o sistemas tecnológicos constituyan medidas de vigilancia masiva o indiscriminada, comprometan de manera masiva la seguridad e integridad de los sistemas de comunicación o no cuenten con medidas suficientes para garantizar la auditoría y trazabilidad de su uso por parte de la autoridad judicial federal correspondiente o de otras autoridades con facultades de**

	supervisión, fiscalización o investigación competentes. **II. Las personas fabricantes, desarrolladoras o prestadoras finales de los servicios, equipos o sistemas tecnológicos posean un impedimento legal o contractual para colaborar con las autoridades competentes para investigar conductas relacionadas con el uso ilegal de los servicios, equipos o sistemas tecnológicos.** **III. El solicitante, sus subsidiarias, filiales o las personas fabricantes, desarrolladoras o prestadoras finales de los servicios, equipos o sistemas tecnológicos, comercialicen, por sí o por interpósita persona, los servicios, equipos o sistemas tecnológicos en países que, a juicio de la Secretaría, se cometan violaciones sistemáticas a los derechos humanos.** **IV. En el país de origen de las personas fabricantes, desarrolladoras o prestadoras finales de los servicios, equipos o sistemas tecnológicos a los que se refiere este título, se cometan violaciones sistemáticas a los derechos humanos o representen una amenaza a la seguridad nacional, a juicio de la Secretaría.** **Artículo 156.- La Secretaría mantendrá un registro de las personas autorizadas para comercializar equipos o sistemas tecnológicos para la intervención de comunicaciones privadas o la geolocalización de equipos de comunicación móvil.** **El registro incluirá por lo menos lo siguiente:** **I. Nombre o razón social de la persona autorizada.** **II. Domicilio y teléfono.** **III. Número o registro de autorización otorgado.** **IV. Fecha de autorización.** **V. Nombre comercial y descripción general de los equipos o sistemas tecnológicos comercializados.** **VI. Nombre o razón social de las personas fabricantes, desarrolladoras o prestadoras finales del servicio, equipo o sistema tecnológico comercializado.** **VII. En su caso, país de origen de las**

	personas a las que se refiere el párrafo anterior. **VIII. La información adicional que determine la Secretaría.** **Artículo 157.- El incumplimiento de las disposiciones de este título, dará lugar a que la utilización de equipos y sistemas tecnológicos para la intervención de comunicaciones privadas o la geolocalización en tiempo real de equipos de comunicación móvil se considere ilegal y sea sancionada en los términos de las normas aplicables.** **La autorización previamente otorgada será revocada cuando dejen de cumplirse los requisitos que fueron necesarios para obtenerla.**

I. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público

LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO	PROPUESTA DE REFORMA
Artículo 50.- Las dependencias y entidades se abstendrán de recibir proposiciones o adjudicar contrato alguno en las materias a que se refiere esta Ley, con las personas siguientes: (...) XV. Las demás que por cualquier causa se encuentren impedidas para ello por disposición de Ley.	**Artículo 50.-** Las dependencias y entidades se abstendrán de recibir proposiciones o adjudicar contrato alguno en las materias a que se refiere esta Ley, con las personas siguientes: (...) **XIV. Las que incumplan con los requisitos a los que se refieren los artículos 153 a 157 de la Ley General del Sistema Nacional de Seguridad Pública.** **XV.** Las demás que por cualquier causa se encuentren impedidas para ello por disposición de Ley.
Artículo 60. La Secretaría de la Función Pública, además de la sanción a que se refiere el primer párrafo del artículo anterior, inhabilitará temporalmente para participar de manera directa o por interpósita persona en procedimientos de contratación o celebrar contratos regulados por esta Ley, a las personas que se encuentren en alguno de los supuestos siguientes: (...) V. Las que se encuentren en el supuesto de la fracción XII del artículo 50 de este ordenamiento, y	**Artículo 60.** La Secretaría de la Función Pública, además de la sanción a que se refiere el primer párrafo del artículo anterior, inhabilitará temporalmente para participar de manera directa o por interpósita persona en procedimientos de contratación o celebrar contratos regulados por esta Ley, a las personas que se encuentren en alguno de los supuestos siguientes: V. Las que se encuentren en el supuesto de la fracción XII del artículo 50 de este ordenamiento, ~~y~~ VI. Aquéllas que se encuentren en el supuesto del

VI. Aquéllas que se encuentren en el supuesto del segundo párrafo del artículo 74 de esta Ley. (...)	segundo párrafo del artículo 74 de esta Ley**, y** **VII. Aquéllas que se encuentren en el supuesto de la fracción XIV del artículo 50 de este ordenamiento.** (...)

J. Ley General de Transparencia y Acceso a la información Pública

LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA	PROPUESTA DE REFORMA
Artículo 70. En la Ley Federal y de las Entidades Federativas se contemplará que los sujetos obligados pongan a disposición del público y mantengan actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan: I a XLVI (...) XLVII. Para efectos estadísticos, 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, y XLVIII (...) (...)	**Artículo 70.** En la Ley Federal y de las Entidades Federativas se contemplará que los sujetos obligados pongan a disposición del público y mantengan actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan: I a XLVI (...) XLVII. Para efectos estadísticos, el listado de ~~solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de Internet para~~ **información relacionada con** la intervención de comunicaciones privadas, **la extracción de información,** el acceso ~~**al registro de comunicaciones**~~ **a datos conservados** 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, y**~~ **de manera desagregada, incluya lo siguiente, de conformidad con el formato que elabore el Instituto:** **Respecto de las autoridades facultadas para llevar a cabo las medidas a las que se refiere esta fracción:**

	a. El número total y, en su caso, por concesionario y autorizado de telecomunicaciones, así como por proveedor de aplicaciones, contenidos y servicios en Internet, de las medidas de intervención de comunicaciones privadas de extracción de datos, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando el número de solicitudes realizadas, autorizadas y no autorizadas mensualmente, así como las que de manera excepcional fueron realizadas sin previa autorización judicial, de las cuales deberá indicarse el número de medidas ratificadas parcial o totalmente o no ratificadas por parte del Juez de control. **b. El número total, por objeto y fundamento legal, de medidas de intervención de comunicaciones privadas de extracción de datos, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando el número de solicitudes realizadas, autorizadas y no autorizadas mensualmente, así como las que de manera excepcional fueron realizadas sin previa autorización judicial, de las cuales deberá indicarse el número de medidas ratificadas parcial o totalmente o no ratificadas por parte del Juez de control.**

	En el caso de autoridades de seguridad pública, interior o de procuración de justicia se entenderá por objeto, los delitos que investigados en el expediente o carpeta de investigación que ameritan la solicitud. **En el caso del Centro Nacional de Inteligencia, se entenderá por objeto, el inciso del artículo 5 de la Ley de Seguridad Nacional aplicable a la amenaza que amerita la solicitud.** **c. El número total, por medida, de personas, líneas, cuentas o dispositivos objeto de las medidas llevadas a cabo mensualmente.** **Respecto de la autoridad judicial que conozca de las solicitudes de autorización de las medidas a las que se refiere esta fracción:** **d. El número total, por autoridad solicitante, y en su caso, por concesionario y autorizado de telecomunicaciones, así como por proveedor de aplicaciones, contenidos y servicios en Internet, cuya colaboración se solicita, de las solicitudes de autorización de medidas de intervención de comunicaciones privadas de extracción de datos, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando el número de solicitudes realizadas, autorizadas y no**

	autorizadas mensualmente, así como las que de manera excepcional fueron realizadas sin previa autorización judicial, de las cuales deberá indicarse el número de medidas ratificadas parcial o totalmente o no ratificadas por parte del Juez de control competente. **e. El número total, por objeto y fundamento legal, de las solicitudes de autorización de medidas de intervención de comunicaciones privadas de extracción de datos, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando el número de solicitudes realizadas, autorizadas y no autorizadas mensualmente, así como las que de manera excepcional fueron realizadas sin previa autorización judicial, de las cuales deberá indicarse el número de medidas ratificadas parcial o totalmente o no ratificadas por parte del Juez de control.** **En el caso de autoridades de seguridad pública, interior o de procuración de justicia se entenderá por objeto, los delitos que investigados en el expediente o carpeta de investigación que ameritan la solicitud.** **En el caso del Centro Nacional de Inteligencia, se entenderá por objeto, el inciso del artículo 5 de la Ley de Seguridad Nacional aplicable a la amenaza que amerita la**

	solicitud. **f. El número total, por medida, de personas, líneas, cuentas o dispositivos objeto de las medidas autorizadas mensualmente.** XLVIII (...) (...)

K. Ley Federal de Transparencia y Acceso a la Información Pública

LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA VIGENTE	PROPUESTA DE REFORMA
Artículo 69. Además de lo señalado en el artículo anterior, los sujetos obligados del Poder Ejecutivo Federal, deberán poner a disposición del público y actualizar la siguiente información: I a IV (...) V. En materia de seguridad pública y procuración de justicia: a) Para efectos estadísticos, 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; b) a e) (...) VI a XV (...)	**Artículo 69.** Además de lo señalado en el artículo anterior, los sujetos obligados del Poder Ejecutivo Federal, deberán poner a disposición del público y actualizar la siguiente información: I a IV (...) V. En materia de seguridad pública y procuración de justicia: a) Para efectos estadísticos, el listado de ~~solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de Internet para~~ **información relacionada con** la intervención de comunicaciones privadas, **la extracción de información,** el acceso ~~**al registro de comunicaciones**~~ **a datos conservados** 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, y**~~ **de manera desagregada, incluya lo siguiente, de conformidad con el formato que elabore el Instituto:** **El número total y, en su caso, por concesionario y autorizado de telecomunicaciones, así como por proveedor de aplicaciones, contenidos**

	y servicios en Internet, de las medidas de intervención de comunicaciones privadas de extracción de datos, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando el número de solicitudes realizadas, autorizadas y no autorizadas mensualmente, así como las que de manera excepcional fueron realizadas sin previa autorización judicial, de las cuales deberá indicarse el número de medidas ratificadas parcial o totalmente o no ratificadas por parte del Juez de control. **El número total, por objeto y fundamento legal, de medidas de intervención de comunicaciones privadas de extracción de datos, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando el número de solicitudes realizadas, autorizadas y no autorizadas mensualmente, así como las que de manera excepcional fueron realizadas sin previa autorización judicial, de las cuales deberá indicarse el número de medidas ratificadas parcial o totalmente o no ratificadas por parte del Juez de control.** **En el caso de autoridades de seguridad pública, interior o de procuración de justicia se entenderá por objeto, los delitos investigados en el expediente o carpeta de investigación que ameritan la solicitud.** **En el caso del Centro Nacional de Inteligencia, se entenderá por objeto, el inciso del artículo 5 de la Ley de Seguridad Nacional aplicable a la amenaza que amerita la solicitud.** **El número total, por medida, de personas, líneas, cuentas o dispositivos objeto de las medidas llevadas a cabo mensualmente.** b) a e) (...) VI a XV (...)

Artículo 71. Además de lo señalado en el artículo 73 de la Ley General y 68 de esta Ley, los sujetos obligados del Poder Judicial Federal deberán poner a disposición del público y actualizar la siguiente información: (...)	**Artículo 71.** Además de lo señalado en el artículo 73 de la Ley General y 68 de esta Ley, los sujetos obligados del Poder Judicial Federal deberán poner a disposición del público y actualizar la siguiente información: (...) IX. Para efectos estadísticos, el listado de **información relacionada con** la intervención de comunicaciones privadas, **la extracción de información,** el acceso **a datos conservados** y la localización geográfica en tiempo real de equipos de comunicación, que **de manera desagregada, incluya lo siguiente, de conformidad con el formato que elabore el Instituto:** **A. El número total, por autoridad solicitante, y en su caso, por concesionario y autorizado de telecomunicaciones, así como por proveedor de aplicaciones, contenidos y servicios en Internet, cuya colaboración se solicita, de las solicitudes de autorización de medidas de intervención de comunicaciones privadas de extracción de datos, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando el número de solicitudes realizadas, autorizadas y no autorizadas mensualmente, así como las que de manera excepcional fueron realizadas sin previa autorización judicial, de las cuales deberá indicarse el número de medidas ratificadas parcial o totalmente o no ratificadas por parte del Juez de control competente.** **B. El número total, por objeto y fundamento legal, de las solicitudes de autorización de medidas de intervención de comunicaciones privadas de extracción de datos, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando el número de solicitudes realizadas, autorizadas y no autorizadas mensualmente, así como las que de manera excepcional fueron realizadas**

	sin previa autorización judicial, de las cuales deberá indicarse el número de medidas ratificadas parcial o totalmente o no ratificadas por parte del Juez de control. **En el caso de autoridades de seguridad pública, interior o de procuración de justicia se entenderá por objeto, los delitos investigados en el expediente o carpeta de investigación que ameriten la solicitud.** **En el caso del Centro Nacional de Inteligencia, se entenderá por objeto, el inciso del artículo 5 de la Ley de Seguridad Nacional aplicable a la amenaza que amerita la solicitud.** **C. El número total, por medida, de personas, líneas, cuentas o dispositivos objeto de las medidas autorizadas mensualmente.**

L. Transitorios

ARTÍCULOS TRANSITORIOS PROPUESTOS
Primero.- El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.
Segundo.- La Federación y entidades federativas competentes dispondrán de 90 días naturales para establecer los registros a los que se refieren los artículos 124, 125 y 156 de la Ley General del Sistema Nacional de Seguridad Pública, relacionados a los equipos y sistemas tecnológicos para la intervención de comunicaciones privadas o la geolocalización en tiempo real de equipos de comunicación móvil.
Tercero.- Las reformas a los párrafos segundo y tercero del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión entrarán en vigor en un plazo de tres años a partir de la publicación del presente Decreto.
Cuarto.- El Instituto Federal de Telecomunicaciones (o la autoridad que sea designada para ejercer sus facultades) modificará los Lineamientos de Colaboración en Materia de Seguridad y Justicia en un plazo de 180 días contado a partir de la publicación del presente Decreto.
Quinto. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (o la autoridad que sea designada para ejercer sus facultades) modificará las disposiciones reglamentarias para instrumentar las obligaciones de transparencia a que se refiere el artículo 70 de la LGTAIP en un plazo de 180 días contado a partir de la publicación del presente Decreto.
Sexto. El Órgano de Administración Judicial modificará las disposiciones reglamentarias correspondientes para instrumentar las obligaciones de transparencia a que se refiere el

artículo 70 de la LGTAIP en un plazo de 180 días contado a partir de la publicación del presente Decreto.
Séptimo. La información estadística que produzcan las autoridades facultadas, el Poder Judicial Federal y los particulares que colaboren en la intervención de comunicaciones privadas, la extracción de información, el acceso a datos conservados o la geolocalización en tiempo real deberá ser comparable entre sí respecto de las categorías de datos y temporalidad. Para ello, se adoptarán las categorías de datos y temporalidades establecidas en la LGTAIP y la LFTR.
Octavo.- Queda derogada cualquier disposición que contravenga los principios, bases, procedimientos y derechos reconocidos en la presente Ley, sin perjuicio de lo previsto en los siguientes Transitorios.
Noveno.- Las autoridades correspondientes deberán adecuar su normatividad interna y reglamentaria, de conformidad con lo que señala el presente Decreto, dentro de un plazo de 180 días a partir de su publicación.