Un marco jurídico de derechos humanos para la vigilancia de las comunicaciones en América Latina

Argentina, Brasil, Chile, Colombia,
México, Panamá, Paraguay y Perú

AlSur

Un marco jurídico de derechos humanos para
la vigilancia de las comunicaciones en América Latina
Argentina, Brasil, Chile, Colombia, México, Panamá, Paraguay y Perú.

Marzo, 2021.

Este documento fue hecho desde **Al Sur** gracias al Fondo INDELA.

Autoría: **Juan Camilo Rivera** y **Carolina Botero** para Al Sur.

AlSur es un consorcio de organizaciones que trabajan en la sociedad civil y en el ámbito académico en América Latina y que buscan con su trabajo conjunto fortalecer los derechos humanos en el entorno digital de la región. Para más información sobre Al Sur y sus miembros, visite https://www.alsur.lat/

Tabla de contenidos

I. Introducción

La vigilancia de las comunicaciones es una herramienta útil para los Estados en su lucha contra el terrorismo y la delincuencia organizada. Su regulación ha planteado siempre retos relacionados, entre otros, al secreto en el que se desarrollan y a la evolución de los mecanismos mediante los cuales se lleva a cabo.

Es necesario reconocer que las tecnologías digitales han aumentado la forma como estas actividades de vigilancia pueden interferir con derechos fundamentales como la libertad de expresión y la privacidad de datos personales, así como afectar el ejercicio de otros derechos importantes en una democracia como los de asociación y libre desarrollo de la personalidad.

En este contexto, los diferentes actores sociales deben mantener abiertos los debates sobre el impacto de las actividades de vigilancia en América Latina, especialmente en materia de derechos humanos. Estas discusiones deben servir para identificar y fortalecer líneas de investigación y discusión de políticas públicas, especialmente en relación con las actividades de vigilancia masiva facilitadas por los avances tecnológicos y que son ejecutadas por los propios Estados o, cada vez más, a través de sus poderes para tener acceso ilimitado a los datos personales en manos del sector privado. En un entorno fuertemente marcado por las tecnologías es necesario discutir el impacto a los derechos de los avances tecnológicos, que, así como ofrecen nuevas formas de enfrentar las amenazas a la seguridad y estabilidad de las sociedades, también las incrementan.

Adoptar y ajustar los marcos jurídicos de los Estados a los estándares internacionales de respeto a los derechos de las personas es un reclamo recurrente de los últimos años, encaminado no solo a ajustar las facultades, sino también con el fin de garantizar mecanismos efectivos de control y seguimiento, y de contar con acciones judiciales y extrajudiciales de cumplimiento.

La necesidad de imponer límites a las facultades de vigilancia fue abordada por los relatores especiales de libertad de expresión de los diferentes organismos internacionales ya en 2013 en su Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión[1]. En foros como el de la Organización para la Cooperación y el Desarrollo Económico (OECD)[2], que se encuentra ajustando sus Directrices de Privacidad, y está analizando el tema del acceso ilimitado de los gobiernos a los datos personales en poder de las empresas dónde seguramente discutirán mecanismos de seguimiento y control para estas facultades, incluyendo la estandarización de informes de transparencia tanto por privados como por gobiernos. Finalmente, las investigaciones de organismos como la European Union Agency for Fundamental Rights (FRA) han establecido que en temas de vigilancia el derecho de las personas a solicitar una reparación es limitado y difícil pero no inexistente,al punto que recuerda cómo en 2010 el informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo afirmó que "las personas afectadas por las acciones ilegales de un servicio de inteligencia pueden recurrir a una institución que

1 Puede consultarse en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927

2 En diciembre de 2020 la OCDE publicó una declaración sobre este tema en la que establece la creación de un grupo para trabajar recomendaciones para sus estados miembros http://www.oecd.org/sti/ieconomy/trusted-government-access-personal-data-private-sector.htm

les proporcione un recurso efectivo, incluida la plena reparación del daño sufrido" y explicó la forma como en Europa avanza en la práctica[3].

¿Cuál es la situación actual del marco jurídico de la vigilancia de las comunicaciones en América Latina? Esa es la pregunta que da sustento a este primer análisis enfocado en las actividades de investigación criminal y de inteligencia. Contar con una línea base comparativa de países de la región nos permitirá abordar los debates e investigaciones regionales para mantener un marco jurídico respetuoso de los derechos de las personas, garante en sus prácticas y con mecanismos de control y seguimiento efectivos que les permita reclamar la restitución de los derechos y sirva como control democrático a los amplios poderes de los Estados en este tema.

Con este propósito, el análisis se basa en el marco jurídico de la vigilancia de las comunicaciones en ocho países de América Latina: Argentina, Brasil, Chile, Colombia, México, Panamá, Paraguay y Perú.[4] Particularmente, estudia el régimen del acceso a las comunicaciones privadas por parte del Estado en dos circunstancias específicas: (i) las investigaciones que se realizan en el marco de un proceso penal y (ii) el ejercicio de labores de inteligencia y contrainteligencia.

El documento recoge un análisis comparado de los sistemas jurídicos de los ocho países, algunas recomendaciones para mejorarlo y presenta detalles del análisis realizado en cada país advirtiendo algunas diferencias en la regulación que cada jurisdicción ha elegido. El análisis se basa en la descripción del marco legislativo doméstico, que se presenta en el siguiente capítulo, teniendo en cuenta en cada caso los mismos ejes temáticos.

Con relación a cada país se estudiaron tres temas:

- Descripción general del marco constitucional de la vigilancia de las comunicaciones, en particular de la manera cmo las constituciones reconocen el derecho a la intimidad y al secreto de las comunicaciones, las circunstancias específicas en las que se habilita su limitación y el procedimiento que debe seguirse para ese propósito. Igualmente, de ser el caso, se explica el lugar que las constituciones les asignan a los tratados internacionales sobre derechos humanos en el ordenamiento jurídico interno, pues ello puede complementar el marco jurídico de protección del derecho a la inviolabilidad de las comunicaciones privadas.

- En lo que tiene que ver con las labores de inteligencia, se presentan los siguientes aspectos del régimen jurídico: (i) autoridades que pueden realizar labores de inteligencia; (ii) definición de las labores de inteligencia y contrainteligencia; (iii) facultades de las autoridades de inteligencia que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones; (iv) procedimiento para el ejercicio de tales facultades; y (v) controles a las labores de inteligencia.

---

3 El estudio "Surveillance by intelligence services – Volume II: field perspectives and legal updateFRAFREEDOMSSurveillance by intelligence services: fundamental rights safeguards and remedies in the EUVolume II: field perspectives and legal update" puede consultarse en https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf

4 La razón de la elección de estos países es porque, hasta el 2020, esos son los países base a los que los miembros de AI Sur pertenecen.

- Con relación a la vigilancia de las comunicaciones en el marco de procesos penales, se abordan 5 temas: (i) autoridades que pueden ordenar la vigilancia; (ii) facultades de las autoridades de investigación penal que interfieren con las comunicaciones personales; (iii) hipótesis en las que tales facultades pueden ejercerse; (iv) procedimiento que debe seguirse para que se ordene una actuación de vigilancia de comunicaciones; y (v) controles para prevenir el ejercicio abusivo de la vigilancia de las comunicaciones.

Alcance del documento y metodología

Teniendo en cuenta el propósito descrito, algunas aclaraciones resultan de especial importancia. Al centrarse en el análisis de las normas sobre vigilancia de las comunicaciones en la jurisdicción de cada país, no se pretende sugerir que este sea el único aspecto relevante para garantizar el derecho a la confidencialidad de las comunicaciones privadas. Es claro que este estudio debe complementarse con otros que analicen el grado de cumplimiento de la legislación interna por las autoridades correspondientes. En todo caso, se considera que la descripción de los marcos normativos nacionales es útil para identificar responsabilidades en la adecuada protección de la confidencialidad de las comunicaciones privadas.

En segundo lugar, el propósito del documento es realizar una descripción uniforme de los distintos marcos jurídicos analizados, para lo cual se seleccionaron algunos temas. Con todo, este ejercicio tiene limitaciones, por diferentes razones, entre las cuales se encuentra que no todos los sistemas jurídicos describen con el mismo grado de precisión los distintos temas abordados en el estudio.

Finalmente, conviene también mencionar que los marcos normativos cambian con el tiempo, por lo que debe tenerse bien presente que el propósito del documento es describir la situación normativa de los ocho países mencionados a diciembre del 2020, invitando a recordar que para el momento de consultar este documento la regulación nacional puede haber cambiado o puede haber propuestas orientadas a ello.

II. La vigilancia de las comunicaciones en América Latina, un marco jurídico en construcción

La constitución política de cada uno de los países objeto del presente estudio protege el derecho al secreto de las comunicaciones, agregando siempre algunas garantías encaminadas a protegerlo. Común a todas ellas es la exigencia que este derecho puede limitarse solo en los casos expresamente previstos en la ley. Algunas constituciones incluyen garantías más específicas, como la exclusión de valor probatorio a documentos obtenidos sin cumplir la reserva judicial y legal de las comunicaciones, consagrada en la Constitución de Perú, o el deber de identificar de forma precisa en la solicitud de interceptación de comunicaciones a la persona afectada, la duración y los medios empleados, prevista en la Constitución de México.

El marco constitucional de la vigilancia de comunicaciones en los ochos países estudiados debe tener en cuenta la jerarquía que en el sistema de fuentes de derecho se les otorga a los tratados internacionales, por cuanto tales instrumentos internacionales, así como que los pronunciamientos de organismos internacionales que los han aplicado, contienen garantías adicionales a la confidencialidad de las comunicaciones. En ese sentido, es relevante señalar que, con ciertas particularidades que deben ser tenidas en cuenta en cada caso, Argentina, Brasil, Chile, Colombia y México, expresamente se prevé la posibilidad de que al menos algunos tratados internacionales sobre derechos humanos tienen jerarquía constitucional.

En materia de inviolabilidad de las comunicaciones por la realización de actividades de inteligencia, todos los países estudiados, con excepción de Panamá, han promulgado leyes que pretenden organizar y sistematizar el andamiaje jurídico para la realización de labores de inteligencia.

Los sistemas jurídicos de los países estudiados suelen consagrar límites que deben guiar la realización de labores de inteligencia. En ocasiones estos límites están formulados de forma general, indicando tan solo que ellas deben respetar la Constitución y/o los derechos fundamentales (como sucede en los casos de Chile y México), mientras que en otros casos están previstas de manera expresa con un poco más de detalle, haciendo referencia, por ejemplo, a la no discriminación en el ejercicio de labores de inteligencia (como es el caso de Argentina, Colombia y Paraguay) y a no interferir en la vida interna institucional, económica y política (como sucede en Argentina y Paraguay).

Por otra parte, el tipo de facultades permitidas para los organismos que llevan a cabo labores de inteligencia tiene variaciones importantes. La más destacable es que algunos países facultan a los organismos de inteligencia a la realización de interceptaciones de comunicaciones telefónicas, mientras que otros no incluyen esta como una de las atribuciones propias de las labores de inteligencia. En la primera categoría se encuentran Argentina, Chile, México, Paraguay y Perú. Es preciso resaltar que en todos estos casos se consagra que debe existir autorización judicial previa para que se proceda a la interceptación de comunicaciones con fines de inteligencia.

Por último, para controlar el ejercicio de las labores de inteligencia cada legislación establece distintos controles. Algunos de esos controles operan respecto de facultades específicas atribuidas a esos organismos, como sucede con relación a la interceptación de comunicaciones telefónicas en aquellos países donde ella es una atribución de los organismos de inteligencia (es decir, Argentina, Chile, México, Paraguay y Perú), según se indicó antes. En tal caso, procede el control judicial de forma previa. Otros controles operan con relación al funcionamiento en su conjunto de las funciones de inteligencia. Entre ellos, el más común es el establecimiento de un organismo en el órgano legislativo respectivo que fiscalice las labores de inteligencia. Así sucede en el caso de Argentina, Brasil, Chile, Colombia, México y Paraguay. En ocasiones la ley no define con precisión el alcance de tal control, como sucede en el caso de Brasil, donde se indica que en un acto posterior del poder legislativo definirá su alcance. Es destacable que en algunos países este control no solo tiene la competencia de conocer los informes que los organismos de inteligencia les presenten, sino que también puede solicitar información con el fin de cumplir las funciones encomendadas, como sucede en Argentina y Perú.

Por su parte, en lo que tiene que ver con la limitación a la inviolabilidad de las comunicaciones para fines de investigación penal, la regulación de los países estudiados en el informe presenta más similitudes entre sí. En términos generales, puede afirmarse que se faculta a las autoridades a interceptar las comunicaciones privadas cuando ello sea relevante para la investigación de delitos. Debe mencionarse que en el caso de México tal facultad se reconoce no sólo para la investigación de delitos sino también para su prevención, por lo que se le permite a la Guardia Nacional solicitar la interceptación de comunicaciones.

El grado de detalle de la regulación de esta medida en los ocho países objeto de este estudio varía, incluyendo los casos de México y Paraguay, donde no hay una regulación concreta de la interceptación de comunicaciones en las actividades de investigación penal. Entre las restantes, en algunas legislaciones se restringe la procedencia de la interceptación de comunicaciones para ciertos delitos, estableciendo un umbral de gravedad reflejado en la pena mínima con la que se sanciona un delito para que en su investigación pueda ordenarse esa medida. Así sucede en los casos de Brasil, Chile y Perú. La duración de la medida varía también: las más cortas son de 15 y 20 días, en Brasil y Panamá, respectivamente, en ambos casos prorrogables, mientras que la más extensa es la de Colombia, donde se permite que se conceda hasta por 3 meses, prorrogables.

Adicionalmente, ciertas legislaciones incluyen otros medios de investigación que también limitan la inviolabilidad de las comunicaciones a través de otras vías. Por ejemplo, en Brasil se faculta la captura ambiental de señales electromagnéticas, ópticas o acústicas, o en México se habilita a las autoridades a proceder a la geolocalización y a solicitar la entrega de datos conservados. Mientras que en Colombia se habla de “monitoreo del espectro”.

El control que procede para la realización de la interceptación de comunicaciones es judicial y previo a su realización. La excepción a esta regla es Colombia, donde se prevé que la realización de interceptación de comunicaciones será ordenada directamente por la Fiscalía General de la Nación y sometida a control judicial posterior, dentro de las 24 horas siguientes al diligenciamiento de las órdenes correspondientes.

Ahora bien, existen otras facultades distintas a la interceptación de comunicaciones que pueden ejercerse en el marco de actividades de investigación penal que también limitan la confidencialidad de las comunicaciones y que no requieren control judicial previo. Así sucede en el caso de México con relación a la geolocalización y la entrega de datos conservados, caso en el cual sí existe control judicial, pero posterior. Igualmente, la legislación brasileña establece el deber de concesionarias de telefonía móvil y fija de poner a disposición del jefe de la Policía Civil y la Fiscalía General (en portugués, "Ministério Público") *los registros para identificar los números de terminales entrantes y salientes de llamadas internacionales, de larga distancia o locales*. El ejercicio de esta función no requiere de control judicial.

Un aspecto único y destacable es que la legislación chilena establece que la medida de interceptación de comunicaciones debe notificarse a la persona contra la que se dirigió una vez esta ha sido realizada y siempre y cuando ello no pusiera en peligro la vida o la integridad de terceras personas.

III. La hoja de ruta para los países de América Latina debe ser el cumplimiento de los derechos humanos en las labores de vigilancia de las comunicaciones

Los marcos jurídicos de distintos países de la región han logrado cierto nivel de estandarización en materia de limitar las facultades de vigilancia de las comunicaciones para garantizar los derechos humanos. Así, por ejemplo, se cuenta con una protección constitucional generalizada a la privacidad. Tal protección es desarrollada de forma detallada por la legislación, por lo general de forma más amplia y específica en materia de vigilancia criminal que en la de inteligencia.

En términos generales en materia de facultades encontramos unos marcos jurídicos diseñados para la era pre-internet. Las normas de América Latina en general todavía no abordan los retos ya reconocidos en las actividades de vigilancia masiva, dejando el alcance de estas facultades a la interpretación judicial en temas como retención de datos, acceso directo a las infraestructuras de las comunicaciones, las facultades en relación con las fuentes de inteligencia abierta o las capacidades de las autoridades de inteligencia para "hackear" dispositivos. Tampoco se han actualizado las normas en materia de cooperación internacional.

Habría que mencionar algunas excepciones —que en todo caso son vagas. En México existen previsiones mínimas sobre geolocalización y entrega de datos conservados, mientras que en las legislaciones de Brasil y Colombia se encuentran conceptos vagos como "captura ambiental de señales electromagnéticas" o "monitoreo del espectro". Adicionalmente, en temas como el de cooperación internacional, que se debaten a nivel internacional, la asignatura en la región está pendiente.

En materia de control y seguimiento a los amplios poderes de vigilancia de las comunicaciones en materia de inteligencia, los más comunes son políticos y en general las leyes son muy generales al definirlo, y solo algunas han establecido expresamente que quienes pueden hacer estos controles están facultados para, por ejemplo, pedir información adicional. De nuevo, en México se han establecido algunos controles en los temas de geolocalización y conservación de datos, pero son posteriores. Como una medida excepcional, hemos calificado el hecho de que en Chile se haya previsto la obligación de notificar a las personas que son objeto de una interceptación de comunicaciones dentro de un contexto concreto.

El alcance de esta investigación no permite evaluar la eficacia de ninguno de estos mecanismos de seguimiento y control, pero el panorama se siente pobre si consideramos que en Europa para el caso de inteligencia, que suele ser más críptico, además de que es popular el control parlamentario (político), hay recursos judiciales y aumentan los países en donde se asignan las facultades de seguimiento y control de estas actividades a organismos independientes en donde el rol de la transparencia y el escrutinio público aumenta[5]. Por ejemplo, aunque en algunos países las autoridades de protección de datos no tienen facultades en este campo, en otros sí y en varios tienen en este tema las mismas facultades que en cualquier otro.

Finalmente, en materia de acciones judiciales o extrajudiciales que permitan a las personas hacer exigibles sus derechos, es un tema que no tiene desarrollo legal expreso en la región. Es decir, se podrán usar acciones ya existentes, como intentar controles usando el régimen de protección de datos, usando peticiones de habeas data para establecer si las autoridades pidieron sus datos, y luego buscan con acciones generales dar aplicabilidad a las protecciones constitucionales. Pero no hay rutas expresas que apoyen un proceso de este tipo.

Para lograr un marco jurídico adecuado a esta época los actores de la región debemos trabajar para:

1. Buscar un marco jurídico que garantice facultades de vigilancia de las comunicaciones legales con el fin de que estas se ejerzan sólo cuando sean necesarias y proporcionales. En este sentido, se debe buscar que en su trámite se debatan las garantías necesarias de cara a los retos que representan los nuevos desarrollos tecnológicos.
2. Profundizar en cómo funcionan en la práctica los mecanismos de seguimiento y control que existen actualmente sobre las actividades de vigilancia de las comunicaciones y llevar los marcos jurídicos de la región a estándares internacionales donde estos mecanismos no se limitan al ámbito político.
3. Analizar la viabilidad y requerimientos para trabajar en rutas judiciales e incluso administrativas que permitan garantizar efectividad a la hora de reclamar estos derechos.

5 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf pag 56 y siguientes.

IV. Descripción detallada de la regulación de la vigilancia de las comunicaciones en ocho países de América Latina

Como se mostrará en este estudio, la inviolabilidad de las comunicaciones es un derecho reconocido en diferentes constituciones, así como también en tratados internacionales sobre derechos humanos. Con todo, se ha aceptado que excepcionalmente pueda limitarse, con el propósito de perseguir determinadas finalidades que se consideran especialmente sensibles en una sociedad democrática. Dos asuntos en los que se admite la limitación de la inviolabilidad de las comunicaciones son la persecución penal de delitos y la recolección de información para efectos de ser utilizada en labores de inteligencia.

El presente estudio realiza una descripción del marco jurídico de la inviolabilidad de las comunicaciones, para lo cual aborda tres cuestiones. Primero, se explica la forma como la constitución de cada país regula este derecho. En segundo y tercer lugar, respectivamente, se aborda la manera como operan los dos temas antes mencionados en los que se admite la limitación de la inviolabilidad de las comunicaciones: las labores de inteligencia y contrainteligencia y la investigación de delitos.

Argentina

a. Marco constitucional de la vigilancia de las comunicaciones

El artículo 18 de la Constitución de la Nación Argentina de 1994 establece distintas garantías personales en el marco de un proceso penal. Una de ellas es la inviolabilidad del domicilio, la "correspondencia epistolar" y los "papeles privados". Esa misma norma indica que tal garantía puede ser limitada mediante una ley, la cual deberá indicar los casos y justificativos en los que podrá procederse a su allanamiento y ocupación.

En cuanto al valor normativo de los tratados internacionales, la Constitución señala, en el numeral 22 del artículo 75, que determinados tratados internacionales "tienen jerarquía constitucional". Se trata de los siguientes: "[l]a Declaración Americana de los Derechos y Deberes del Hombre; la Declaración Universal de Derechos Humanos; la Convención Americana sobre Derechos Humanos; el Pacto Internacional de Derechos Económicos, Sociales y Culturales; el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo; la Convención sobre la Prevención y la Sanción del Delito de Genocidio; la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial; la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer; la Convención contra la Tortura y otros Tratos o Penas Crueles, Inhumanos o Degradantes; la Convención sobre los Derechos del Niño".

b. Vigilancia de las comunicaciones en el marco de actividades de inteligencia y contrainteligencia

Las actividades de inteligencia en Argentina se encuentran reguladas por la Ley 25.520, promulgada el 3 de diciembre de 2001. Esta disposición fue actualizada por la Ley 27.126, promulgada el 3 de marzo de 2015 y por el Decreto 214 de 2020. Con base en lo dispuesto por estas normas, la Agencia Federal de Inteligencia expidió el Decreto 1311/2015, aprobando la "Nueva Doctrina de Inteligencia Nacional".

i. **Autoridades que pueden realizar labores de inteligencia y contrainteligencia:** el Sistema de Inteligencia Nacional está conformado por tres organismos: (a) la Secretaría de Inteligencia, que lo dirige; (b) la Dirección Nacional de Inteligencia Criminal, que depende de la Secretaría de Seguridad Interior; y (c) la Dirección Nacional de Inteligencia Estratégica Militar, que depende del Ministro de Defensa (Ley 25.520, artículos 6, 9 y 10).

   La misma Ley establece que una Agencia Federal de Inteligencia es el organismo superior del Sistema de Inteligencia Nacional y lo dirige. Tal agencia depende de la Presidencia de la Nación (Ley 25.520, artículos 7 y 15).

ii. **Definición y límites de las labores de inteligencia:** la regulación legal argentina indica que la inteligencia nacional se refiere a la obtención, reunión, sistematización y análisis de información sobre hechos, riesgos y conflictos que afecten la defensa nacional y la seguridad interior de la nación. Estas dos finalidades de la inteligencia nacional dan lugar a una distinción que realiza la legislación entre dos tipos de inteligencia: la criminal y la estratégica militar. Por su parte, también se definen las actividades de contrainteligencia, entendiendo por ellas las realizadas con el fin de evitar actividades de inteligencia de actores que representan amenazas o riesgos para la seguridad del Estado (Ley 25.520, artículo 2).

   Con el fin de demarcar con mayor claridad el ámbito de las labores de inteligencia, la legislación identifica una serie de actividades que no le es permitido realizar a los entes encargados de ellas. Así, el artículo 4 de la Ley 25.520 dispone que ningún organismo de inteligencia podrá cumplir funciones policiales o de investigación criminal, tener en cuenta en la realización de sus funciones motivaciones discriminatorias, buscar influenciar en la vida política, institucional, militar, social o económica del país, ni revelar o divulgar información adquirida en el ejercicio de sus funciones (salvo que medie orden o dispensa judicial).

iii. **Facultades de las autoridades de inteligencia que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones:** la legislación argentina prevé que en el marco de actividades de inteligencia o contrainteligencia puede realizarse interceptación o captación de comunicaciones privadas de cualquier tipo, disponiendo que para tal efecto será indispensable que exista autorización judicial (Ley 25.520, artículo 18). Esta disposición se complementa con otras, que establecen el deber de las empresas de telecomunicaciones de salvaguardar la confidencialidad de las comunicaciones de sus usuarios (Ley 27.078, artículo 62, literal f), señalando que en todo caso deben "atender los requerimientos en materia de defensa nacional y de seguridad pública formulados por las autoridades competentes" (Ley 27.078, artículo 62, literal i).

iv. **Procedimiento para la realización de estas actividades:** están previstos dos procedimientos diferentes, dependiendo del tipo de actividades a realizar. Por un lado, se dispone que las actividades de inteligencia serán ordenadas por las máximas autoridades de cada organismo, y se señala que en caso de urgencia tales actividades podrán ser iniciadas, debiendo ser informadas de manera inmediata a las autoridades máximas de cada organismo de inteligencia.

Por otro lado, el procedimiento es distinto cuando se requiere realizar interceptaciones o captaciones de comunicaciones privadas de cualquier tipo. En ese caso, se requiere autorización judicial, la cual debe ser solicitada siguiendo estas formalidades: ser solicitada por el Secretario de Inteligencia o por el funcionario a quien este expresamente delegue; formularse por escrito; estar fundada indicando con precisión los números telefónicos o direcciones electrónicas o de cualquier medio cuyas comunicaciones se pretenda captar o interceptar (Ley 25.520, artículos 18 y 19). Deberá solicitarse ante un juez federal y podrá ser concedida por 60 días, prorrogables por 60 más. Vencidos estos plazos, el juez determinará el inicio de la causa o la destrucción y/o el borrado de los soportes correspondientes a las interceptaciones o captaciones que se hubieran autorizado (Ley 25.520, artículo 20).

v. **Controles que pueden ejercerse:** los controles que se prevén al ejercicio de las actividades de inteligencia son de dos tipos: políticos y sancionatorios.

Con relación al control político, existe en el Congreso de la Nación la llamada "Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia". Tiene como propósito fiscalizar que el funcionamiento de las labores de inteligencia se ajuste estrictamente a las normas constitucionales, legales y reglamentarias vigentes, así como también a los lineamientos estratégicos y objetivos generales de la política de inteligencia nacional. La Comisión Bicameral tiene la facultad de requerir a las autoridades del Sistema Nacional de Inteligencia información para el cumplimiento de sus funciones (Ley 25.520, artículo 33).

También puede requerir de la dirección correspondiente de la Procuración General de la Nación y de las empresas que presten servicios telefónicos o de telecomunicaciones de cualquier tipo en Argentina informes que contengan el listado de las interceptaciones y derivaciones que se hayan realizado en un período determinado, para establecer que correspondan con requerimientos judiciales (Ley 25.520, artículo 34).

En cuanto a los controles sancionatorios, se establece que los funcionarios que lleven a cabo actividades de inteligencia que infrinjan los deberes y obligaciones de sus funciones incurren en responsabilidad disciplinaria, sin excluir que también incurran en responsabilidad civil y penal (Ley 25.520, artículo 5 bis). Asimismo, la legislación sanciona ciertos delitos relacionados con las labores de inteligencia, como la interceptación indebida de comunicaciones personales (Ley 25.520, artículo 42), la omisión de destruir o borrar soportes de interceptación de comunicaciones (Ley 25.520, artículo 43) y la realización de labores de inteligencia en incumplimiento del procedimiento previsto en la ley (Ley 25.520, artículo 43 bis).

c. Vigilancia de las comunicaciones en el marco de investigaciones penales

Las medidas de investigación penal que pueden afectar la confidencialidad de las comunicaciones se encuentran reguladas por la Ley 27.063, Código Procesal Penal de la Nación. También la Ley 27.078, de Tecnologías de la Información y las Comunicaciones, contiene provisiones sobre la inviolabilidad de las comunicaciones.

i. **Facultades de las autoridades de investigación que interfieren con las comunicaciones personales:** el Código Procesal Penal de la Nación reconoce la facultad de "interceptación y secuestro de correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a éste, aunque sea bajo nombre supuesto". La Ley de Tecnologías de la Información y las Comunicaciones contiene una definición de la "correspondencia" susceptible de ser materia de intervención de las comunicaciones, aclarando que se refiere a las comunicaciones realizadas a través de las redes y de servicios de telecomunicaciones (Ley 27.078, artículo 5).

ii. **Autoridades que pueden ordenar la vigilancia:** el artículo 143 de la Ley 27063 establece que la intervención de comunicaciones procede "a petición de parte", de lo que se desprende que puede ser solicitada no solo por el Ministerio Público Fiscal sino también por el acusado.

iii. **Circunstancias en las que tales facultades pueden ejercerse:** la interceptación de comunicaciones en el marco de un procedimiento penal puede ordenarse "[s]iempre que resulte útil para la comprobación del delito" (Ley 27.063, artículo 143).

iv. **Procedimiento que debe seguirse para que se ordene una actuación de vigilancia de las comunicaciones:** la solicitud de intervención de comunicaciones debe indicar el plazo de duración que se estime necesario (el cual no podrá ser superior a 30 días, renovables si se justifica teniendo en cuenta la naturaleza y circunstancias del hecho investigado). Al resolverla, el juez deberá analizar la legalidad y razonabilidad y decidirá de forma motivada. La legislación argentina consagra un deber expreso dirigido a las empresas de comunicación de posibilitar el cumplimiento inmediato de la intervención de comunicaciones. También conviene mencionar que la medida de intervención deberá terminar si los elementos de convicción que dieron lugar a ella desaparecieron, si esta alcanzó su objeto o si se venció el plazo (Ley 27.063, artículo 143).

v. **Controles aplicables a la vigilancia de las comunicaciones en materia penal:** conforme a lo señalado anteriormente, solo puede autorizarse la intervención de comunicaciones mediante orden judicial (Ley 27.063, artículo 143, y Ley 27.078, artículo 5).

Brasil

a. Marco constitucional de la vigilancia de las comunicaciones

La Constitución de la República Federativa de Brasil reconoce en su artículo 5, numeral X, los derechos a la intimidad, la vida privada, el honor y la propia imagen, y establece que se garantiza el derecho a la indemnización por daños materiales o morales que pudieran causarse con su vulneración. A su vez, el numeral XI del mismo artículo prevé la inviolabilidad del domicilio, indicando que no podrá accederse a él sin que medie consentimiento del residente, excepto en tres circunstancias: que medio flagrante delito o desastre, para prestar ayuda o, durante el día, mediante resolución judicial. Por su parte, el numeral XII del mismo artículo 5 consagra la inviolabilidad del secreto de "la correspondencia y de las comunicaciones telegráficas, de datos y de las comunicaciones telefónicas". Adicionalmente, agrega que en el caso de esta última solo puede limitarse tal inviolabilidad cuando medie orden judicial y en los casos y formas que establezca la ley tratándose de una investigación penal o para instruir procesos penales.

La constitución brasileña se refiere nuevamente a este asunto al regular el estado de defensa —el cual es, junto con el estado de sitio, los estados de excepción que esa norma prevé. Al respecto, el artículo 136 señala que esta figura puede ser decretada por el presidente con el propósito de preservar o restablecer rápidamente el orden público o la paz social frente a situaciones en las que estos se encuentren amenazados o afectados. En el decreto mediante el que se tome esta determinación el presidente deberá indicar, entre otras cosas, las limitaciones a ciertos derechos, incluyendo el secreto de la correspondencia y el secreto de las comunicaciones telegráficas o telefónicas. De forma similar, con relación al estado de sitio, se indica que durante su vigencia se podrán tomar, contra las personas implicadas, determinadas medidas, incluyendo "restricciones relativas a la inviolabilidad de la correspondencia, al secreto de las comunicaciones, al suministro de informaciones y a la libertad de prensa, radiodifusión y televisión, de conformidad con lo establecido en la ley".

Por otro lado, en cuanto al valor jurídico de los tratados en materia de derechos humanos, el párrafo 3 del artículo 5 establece que "[l]os tratados y convenciones internacionales sobre derechos humanos que se aprueben en cada Cámara del Congreso Nacional, en dos turnos, por tres quintos de los votos de los respectivos miembros, serán equivalentes a las enmiendas constitucionales".

b. Vigilancia de las comunicaciones en el marco de actividades de inteligencia y contrainteligencia

El marco legal de las actividades de inteligencia en Brasil se encuentra previsto en la Ley 9.883 del 7 de diciembre de 1999, la cual instituyó el Sistema Brasilero de Inteligencia y creó la Agencia Brasilera de Inteligencia. A su vez, la organización y funcionamiento del Sistema Brasilero de Inteligencia están regulados en el Decreto 4.376/02.

i. **Autoridades que pueden realizar labores de inteligencia y contrainteligencia:** conforman el Sistema de Inteligencia Brasileño los órganos y entidades de la Administración Pública Federal que puedan, de forma directa o indirecta, producir información de interés para las actividades de inteligencia. De forma especial, forman parte de dicho sistema los órganos responsables de los sectores de defensa nacional, seguridad interna y relaciones internacio-

nales (Ley 9.883/99, artículo 2). El artículo 4 del Decreto 4.376/02 identifica con detalle el listado de órganos que hacen parte del Sistema de Inteligencia Brasileño.

El órgano central del Sistema de Inteligencia Brasileño es la Agencia Brasileña de Inteligencia, la cual hace parte de la Presidencia de la República. Dicha agencia estará encargada de la planificación, ejecución, coordinación, supervisión y control de las actividades de inteligencia del país. Con ese propósito, los órganos que conforman en Sistema de Inteligencia Brasileño deben proporcionar a la Agencia Brasileña de Inteligencia los datos y conocimientos específicos relacionados con la defensa de las instituciones y los intereses nacionales (Ley 9.883/99, artículo 4).

El Sistema de Inteligencia Brasileño funciona a partir de la articulación de los órganos que lo integran. Estos tienen la función de producir información relevante de acuerdo con la Política Nacional de Inteligencia y de intercambiar información necesaria para la producción de conocimientos relacionados con las actividades de inteligencia y contrainteligencia (Decreto 4.376/02, artículo 6).

ii. **Definición y límites de las labores de inteligencia:** el artículo 2 de la Ley 9.883/99 define la inteligencia como "la actividad que tiene por objeto obtener, analizar y difundir conocimientos dentro y fuera del territorio nacional sobre hechos y situaciones de influencia inmediata o potencial en la toma de decisiones y la actuación de gobierno, y sobre la salvaguardia y seguridad de la sociedad y el estado". Por su parte, se entiende que la contrainteligencia hace referencia a la actividad que tiene como propósito neutralizar la inteligencia adversa.

   En lo que se refiere a los límites a las actividades de inteligencia, la Ley 9.883/99 afirma que las actividades de inteligencia deben llevarse a cabo con "respeto irrestrictico por los derechos y garantías individuales, con lealtad a las instituciones que rigen los intereses y la seguridad del Estado" (artículo 3).

iii. **Facultades que tienen estas autoridades que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones:** los representantes de los órganos que hacen parte del Sistema de Inteligencia Brasileño podrán acceder, por medios electrónicos, a las bases de datos de los órganos a los que pertenecen (Decreto 4.376/02, artículo 6 A §4). Aparte de esta facultad, el marco legal en Brasil no especifica los mecanismos a través de los cuales puede recolectarse o producirse información relevante para la realización de las funciones de inteligencia y contrainteligencia.

iv. **Procedimiento para la realización de estas actividades:** como se desprende del numeral anterior, tampoco se establece un procedimiento para la realización de las funciones de inteligencia que puedan afectar con la privacidad de las comunicaciones personales.

v. **Controles que pueden ejercerse:** al Congreso Nacional se le encarga la función de realizar un control a las actividades de inteligencia. Los integrantes de dicho cuerpo de control legislativo son definidos por la Ley 9.883/99 e incluyen representación de la mayoría y de la minoría de ambas cámaras legislativas. De acuerdo con esta norma, las atribuciones específicas de este órgano de control deben ser definidas mediante un acto del Congreso Nacional (artículo 6).

c. Vigilancia de las comunicaciones en el marco de investigaciones penales

Las facultades de investigación en el marco de procedimientos penales que pueden interferir con las comunicaciones personales se encuentran previstas en una ley que regula específicamente este asunto: la Ley de Interceptación Telefónica (Ley 9.296/96). También existen facultades específicas previstas en otras disposiciones, particularmente en la Ley de Organizaciones Criminales (Ley 12.850/13), en la Ley de Crímenes de Lavado de Dinero (Ley 9.613/98, adicionada por la Ley nº 12.683/2012) y en la ley sobre antiterrorismo (Ley 13.260/16).

i. **Facultades de las autoridades de investigación que interfieren con las comunicaciones personales:** la legislación brasileña prevé la interceptación de comunicaciones en un proceso penal o en una investigación criminal, precisando además que su alcance se aplica también a "la interceptación de las comunicaciones que transcurren vía tecnologías de información y medios telemáticos", incluyendo así los datos que circulan por Internet, como los correos electrónicos.

   También con el propósito de investigación o instrucción penal, un juez podrá autorizar la captura ambiental de señales electromagnéticas, ópticas o acústicas, a solicitud de la autoridad policial o del Ministerio Público.

   Además de las mencionadas, la Ley de Organizaciones Criminales establece otras facultades, cuyo ejercicio no requiere orden judicial. Así, contempla el deber de las concesionarias de telefonía móvil y fija de mantener por cinco años a disposición del jefe de la Policía Civil y la Fiscalía General (en portugués, "Ministério Público") "los registros para identificar los números de terminales entrantes y salientes de llamadas internacionales, de larga distancia o locales" (Ley 12.850/13, artículo 17). También se prevé que estas mismas autoridades accedan a cierta información sobre la cuenta que tengan, entre otras entidades, las compañías telefónicas y las proveedoras de internet (Ley 12.850/13, artículo 15, y Ley 9.613/98, artículo 17-B).

ii. **Autoridades que pueden ordenar la vigilancia:** la interceptación de comunicaciones telefónicas o de las comunicaciones que transcurren vía tecnologías de información y medios telemáticos requiere orden judicial, la cual podrá proferirse de oficio o por solicitud (i) de la autoridad de policía, en el caso de una investigación penal, o (ii) del representante de la Fiscalía General, en el caso de investigación penal o de la instrucción de un proceso penal. También requiere orden judicial la captura ambiental de señales electromagnéticas, ópticas o acústicas. En este segundo caso, la autorización se podrá conferir a solicitud de la autoridad policial o del Ministerio Público.

   Las otras facultades del numeral anterior, como ya se indicó, pueden ser solicitadas por el jefe de la Policía Civil y por la Fiscalía General, sin que se requiera orden judicial.

iii. **Circunstancias en las que tales facultades pueden ejercerse:** la interceptación de comunicaciones telefónicas o de las comunicaciones que transcurren vía tecnologías de información y medios telemáticos solo podrán ordenarse cuando se demuestra que su realización es necesaria para la investigación de una infracción penal, indicando los medios que serán empleados (Ley 9.613/98, artículo 4). Además, no podrá ordenarse si no hay indicios de la autoría o participación en una infracción penal; si la prueba puede ser obtenida por otros medios disponibles; y si el hecho investigado constituye una infracción criminal sancionada, como máximo, con pena de detención (Ley 9.613/98, artículo 2).

Por su parte, la captura ambiental de señales electromagnéticas, ópticas o acústicas podrá ordenarse cuando la prueba no pueda realizarse por otros medios disponibles e igualmente efectivos; y existan elementos probatorios razonables de autoría y participación en infracciones penales cuyas penas máximas sean superiores a 4 (cuatro) años o en infracciones penales conexas (Ley 9.613/98, artículo 8 A).

iv. **Procedimiento que debe seguirse para que se ordene una actuación de vigilancia de comunicaciones:** por regla general, la solicitud debe realizarse por escrito (Ley 9.613/98, artículo 4 §1). Una vez presentada, el juez tiene un plazo de 24 horas para decidir (Ley 9.613/98, artículo 4 §2). La decisión deberá ser fundamentada y precisa, indicando la forma de ejecución. Se concederá por un máximo de 15 días, renovables por el mismo tiempo si se comprueba su indispensabilidad (Ley 9.613/99, artículo 5). De ser concedida la solicitud, deberá ser llevada a cabo por la autoridad policial, quien informará a la Fiscalía General. Una vez finalizada la diligencia, la autoridad policial remitirá al juez el resultado de la interceptación, así como un resumen de las operaciones realizadas. Con estos elementos, el juez determinará incorporarlos al proceso, garantizando su confidencialidad (Ley 9.613/98, artículo 8), o en caso de no encontrarlos útiles o que dejen ser serlo para efectos probatorios, dispondrá su destrucción (Ley 9.613/98, artículo 9).

Por su parte, con relación a la captura ambiental de señales electromagnéticas, ópticas o acústicas, la solicitud debe describir en detalle la ubicación y forma de instalación del dispositivo de captura ambiental. Esta se concederá por un plazo no mayor de 15 días, renovable por decisión judicial por períodos iguales, si se acredita la indispensabilidad de la prueba y cuando se presenta actividad delictiva permanente, habitual o continuada. Finalmente, la legislación brasileña advierte que las reglas en materia de interceptación de comunicaciones telefónicas son aplicables de forma subsidiaria la captura de información ambiental (Ley 9.613/98, artículo 8 A).

v. **Controles aplicables a la vigilancia de las comunicaciones en materia penal:** la interceptación de comunicaciones telefónicas requiere de autorización judicial previa. Igualmente, una vez realizada la diligencia de interceptación, el juez debe decidir si los resultados son relevantes para la investigación, existiendo así también un control judicial posterior (Ley 9.613/98, artículos 1y 8 A).

Conviene señalar que la legislación brasileña contempla la existencia de un Sistema Nacional de Control de Interceptación de Comunicaciones (SNCI), creado mediante la Resolución / CNJ No. 59/2009. Está conformado por un panel designado por el Consejo Nacional de Justicia, para la consulta pública de la información relacionada con la comunicación de decisiones sobre interceptaciones telefónicas, de sistemas informáticos y telemática.

También con relación a la captura ambiental de señales electromagnéticas, ópticas o acústicas procede el control judicial previo y posterior (Ley 9.613/98, artículo 8 A).

Chile

a. Marco constitucional de la vigilancia de las comunicaciones

La Constitución Política de la República de Chile de 1980 establece, en el numeral 5 del artículo 19, que el hogar y toda forma de comunicación privada son inviolables. Asimismo, indica que, para limitar este derecho mediante allanamiento del hogar o interceptación, apertura o registro de comunicaciones y documentos privados, debe mediar una ley que especifique los casos y las formas para ese efecto.

Respecto del valor jurídico de los tratados internacionales sobre derechos humanos, el artículo 5 de la Constitución afirma que es deber de las autoridades respetar y promover los derechos reconocidos por la Constitución, "así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes".

b. Vigilancia de las comunicaciones en el marco de actividades de inteligencia y contrainteligencia

Las actividades de inteligencia en Chile se encuentran reguladas por la Ley 19.974.

i. **Autoridades que pueden realizar labores de inteligencia y contrainteligencia:** el Sistema de Inteligencia del Estado está compuesto por el conjunto de órganos que realizan actividades de inteligencia y contrainteligencia que asesoran, de forma coordinada al presidente y a otros niveles superiores de conducción del Estado para proteger la soberanía nacional y preservar el orden constitucional (Ley 19.974, artículo 2). Está conformado por la Agencia Nacional de Inteligencia, la Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional, la Dirección de Inteligencia de las Fuerzas Armadas y las direcciones o jefaturas de inteligencia de las Fuerzas de Orden y Seguridad Pública (Ley 19.974, artículo 3). La coordinación entre estos distintos organismos la realiza el Comité de Inteligencia (Ley 19.974, artículo 6).

   De los mencionados, es la Agencia Nacional de Inteligencia la encargada de producir inteligencia, para lo cual puede recolectar y procesar información. Tales actividades las puede realizar tan solo a partir de fuentes abiertas, según se explica más adelante.

ii. **Definición y límites de las labores de inteligencia:** por actividades de inteligencia se entiende el "proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones". Por su parte, contrainteligencia es definida como "aquella parte de la actividad de inteligencia cuya finalidad es detectar, localizar y neutralizar las acciones de inteligencia desarrolladas por otros Estados o por personas, organizaciones o grupos extranjeros, o por sus agentes locales, dirigidas contra la seguridad del Estado y la defensa nacional" (Ley 19.974, artículo 2).

   A manera de límites a estas actividades, se establece que las actividades de inteligencia deben desarrollarse con apego a la Constitución Política y a las leyes (Ley 19.974, artículo 3).

iii. **Facultades que tienen estas autoridades que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones:** cuando se requiera la obtención de información que no está disponible en fuentes abiertas (es decir, las que son de público conocimiento), los organismos de inteligencia pueden llevar a cabo determinadas actividades, denominadas "procedimientos especiales", a saber: la intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas; la intervención de sistemas y redes informáticos; la escucha y grabación electrónica incluyendo la audiovisual, y la intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información (Ley 19.974, artículo 24).

iv. **Procedimiento para la realización de estas actividades:** los directores o jefes de los organismos de inteligencia solicitaron autorización judicial para iniciar los procedimientos especiales de obtención de información, mencionados en el numeral anterior. La solicitud será decidida por un ministro de la Corte de Apelaciones (Ley 19.974, artículo 25).

v. **Controles que pueden ejercerse:** la legislación chilena en materia de inteligencia prevé dos tipos de controles: internos y externos.

El interno corresponde al jefe o director de cada organismo del Sistema de Inteligencia del Estado, y tiene como función velar por, entre otras, la adecuación de los procedimientos empleados al respecto de las garantías y a las normas legales y reglamentarias (Ley 19.974, artículo 34).

La Ley 19.974 también incluye controles externos, entre los que se destaca el judicial, que, como ya se explicó, procede con relación a los mecanismos especiales de obtención de información. Cuando se solicite autorización para la realización de tales procedimientos, el juez decidirá en audiencia sin la intervención de los afectados ni de terceros. En caso de autorizarlos, "[l]a resolución que autorice el empleo de los mencionados procedimientos deberá incluir la especificación de los medios que se emplearán, la individualización de la o las personas a quienes se aplicará la medida y el plazo por el cual se decreta, que no podrá ser superior a noventa días, prorrogable por una sola vez hasta por igual período". En caso de negarlos, su decisión podrá ser recurrida para que el juez la reconsidere (artículo 28).

Igualmente, se prevé la conformación de un control parlamentario, a cargo de la Cámara de Diputados, la cual deberá constituir una comisión especial encargada de "conocer los informes y antecedentes relativos a las actividades de los servicios y organismos que integran el Sistema de Inteligencia del Estado" (Ley 19.974, artículo 37).

c. Vigilancia de las comunicaciones en el marco de investigaciones penales

Existe una regulación general de las medidas que interfieran en la confidencialidad de las comunicaciones, contenida en la Ley 19.696, mediante la cual se profirió el Código de Procedimiento Penal. Este marco general se complementa con dos leyes específicas: la Ley 18.314, relacionada con la investigación de actos que esa misma ley considera terroristas, y la Ley 20.000, relacionada con el tráfico ilícito de sustancias estupefacientes y sustancias sicotrópicas.

i. **Facultades de las autoridades de investigación que interfieren con las comunicaciones personales:** la legislación procesal penal chilena prevé la realización de distintas medidas que pueden afectar la confidencialidad de las comunicaciones. Se trata de las siguientes: retención e incautación de correspondencia postal, telegráfica o de otra clase y de los envíos dirigidos al imputado o remitidos por él, o de aquéllos de los cuales se presumiera que emanan de él o de los que él pudiere ser el destinatario (Ley 19.696, artículo 218) e interceptación y grabación de las comunicaciones telefónicas o de otras formas de telecomunicación (Ley 19.696, artículo 222).

ii. **Autoridades que pueden ordenar la vigilancia:** corresponde al fiscal del caso solicitar la autorización de las medidas de investigación previamente mencionadas (Ley 19.696, artículos 218 y 222).

iii. **Circunstancias en las que tales facultades pueden ejercerse:** la retención e incautación de correspondencia y de las demás formas de comunicación previstas en el artículo 218 de la Ley 19.696 "cuando por motivos fundados fuere previsible su utilidad para la investigación".

A su vez, el estándar aplicable para la autorización de interceptación de comunicaciones es más alto, pues puede autorizarse "[c]uando existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen, y la investigación lo hiciere imprescindible". A su vez, también se restringe el ámbito personal de la interceptación de comunicaciones, al indicarse que solo podrá afectar al procesado o a personas respecto de quienes existieran sospechas fundadas de que sirven de intermediario en tales comunicaciones o de que prestan sus medios de comunicación al procesado (Ley 19.696, artículo 222).

iv. **Procedimiento que debe seguirse para que se ordene una actuación de vigilancia de comunicaciones:** en materia de retención e incautación de correspondencia, el fiscal podrá conservar solo con aquella que tuviera relación con el objeto de la investigación (Ley 19.696, artículo 218). La ley establece la facultad del juez de garantías de autorizar que cualquier empresa de comunicaciones facilite copias de las comunicaciones transmitidas o recibidas por ellas (Ley 19.696, artículo 219).

En cuanto a la interceptación de comunicaciones, la orden que la apruebe debe indicar el nombre y la dirección del afectado por la medida y señalar la forma de interceptación. Este requisito tiene una excepción tratándose de la investigación de delitos relacionados con tráfico de sustancias estupefacientes y de sustancias sicotrópicas, pues en este caso basta con indicar información que permita individualizar o determinar al afectado por la medida. Adicionalmente, según la regulación general prevista en la Ley 19.696, la interceptación de comunicaciones no podrá exceder de 60 días, prorrogables por períodos iguales si persisten los requisitos que dieron lugar a ella. Se establece que las empresas de telecomunicaciones tienen el deber de dar cumplimiento a la medida y de otorgar a los funcionarios encargados de realizarlas todas las facilidades para tal efecto, así como de guardar un registro actualizado de las direcciones IP y un registro, por un tiempo no menor a un año, de los números IP de las conexiones que realicen sus abonados. También se añade que los funcionarios encargados de realizar la diligencia y los empleados de las mencionadas empresas deberán guardar su confidencialidad (Ley 19.696, artículo 222). Es destacable señalar asimismo que la medida de interceptación de comunicaciones debe notificarse a la persona contra la que se dirigió una vez esta ha sido realizada y siempre y cuando ello no pusiera en peligro la vida o la integridad de terceras personas (Ley 19.696, artículo 224).

v. **Controles aplicables a la vigilancia de las comunicaciones en materia penal:** la legislación penal chilena dispone que toda actuación que prive al procesado de sus derechos, o los restrinja o perturbe, requiere autorización judicial previa por parte del juez de control de garantías. Esta garantía entonces cubre las medidas restrictivas del derecho a la confidencialidad de las comunicaciones explicadas en esta sección (Ley 19.696, artículo 9).

Colombia

a. Marco constitucional de la vigilancia de las comunicaciones

El artículo 15 de la Constitución Política de Colombia reconoce los derechos a la intimidad, el buen nombre y el habeas data. Además, agrega que el derecho a la intimidad puede ser limitado, al indicar que "[l]a correspondencia y demás formas de comunicación privada son inviolables", especificando a continuación que estas pueden ser interceptadas o registradas (i) mediante orden judicial y (ii) en los casos y con las formalidades que establezca la ley. Además, el artículo 28 de la Constitución establece que toda persona es libre, y que por lo tanto el domicilio de ninguna persona puede ser registrado, "sino en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivo previamente definido en la ley".

La Constitución Política establece una excepción a la regla antes indicada. Se trata de la facultad que tiene la Fiscalía General de la Nación de realizar "registros, allanamientos, incautaciones e interceptaciones de comunicaciones" sin orden judicial previa, aunque en todo caso especificando que deberá existir un control de legalidad posterior de la actuación. Esta es la única excepción en la que se admite una restricción del derecho a la intimidad sin orden judicial previa.

Con relación a la naturaleza jurídica de los tratados internacionales en el orden interno, la Constitución Política señala que, en algunos casos, estos tendrán valor constitucional, mientras que en otros tendrán fuerza interpretativa. Así, sucederá lo primero con relación a "los tratados y convenios internacionales ratificados por el Congreso, que reconocen los derechos humanos y que prohíben su limitación en los estados de excepción" (artículo 93, párrafo 1), mientras que se presentará lo segundo para la interpretación de los derechos consagrados en la Constitución, para lo cual deben tenerse en cuenta todos los tratados internacionales sobre derechos humanos ratificados por Colombia (artículo 93, párrafo 2).

b. Vigilancia de las comunicaciones en el marco de actividades de inteligencia y contrainteligencia

Las actividades de inteligencia y contrainteligencia en Colombia están reguladas por la Ley 1621 de 2013. Esta norma ha sido reglamentada por decretos presidenciales, dentro de los que se destaca el Decreto 857 de 2014, el cual, entre otras, define con detalle los organismos encargados de realizar labores de inteligencia y contrainteligencia.

i. **Autoridades que pueden realizar labores de inteligencia y contrainteligencia:** la función de inteligencia y contrainteligencia es llevada a cabo por ciertas dependencias de las Fuerzas Militares (incluyendo el Comando General, el Ejército Nacional, la Armada Nacional y la Fuerza Aérea) y la Policía Nacional, por la Dirección Nacional de Inteligencia (órgano administrativo del Estado colombiano cuyo director o directora es nombrado por el Presidente de la República) y por la Unidad de Información y Análisis Financiero (Ley 1621/13, artículo 3 y Decreto 857 de 2014, artículo 1).

   También se afirma que existirá una Junta de Inteligencia Conjunta, que tendrá la función de producir estimativos de inteligencia y contrainteligencia para el Gobierno nacional (Ley 1621/13, artículos 12 y 13).

ii. **Definición y límites de las labores de inteligencia:** la legislación colombiana define de forma conjunta las labores de inteligencia y contrainteligencia, entendiendo por ellas las que "desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los demás fines enunciados en esta ley" (Ley 1621/13, artículo 2).

A su vez, se establecen límites expresos al ejercicio de estas actividades, a saber: solo pueden ser realizadas con el propósito de proteger determinadas finalidades, señaladas en la propia ley; no pueden ser utilizadas con propósitos discriminatorios; y se indica que al decidirse sobre el inicio de actividades de inteligencia y contrainteligencia debe analizarse que se cumplan los principios de necesidad, idoneidad y proporcionalidad.

iii. **Facultades que tienen estas autoridades que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones:** la legislación colombiana regula expresamente dos facultades que pueden ejercer los organismos de inteligencia para el cumplimiento de sus funciones. La primera de ellas es el monitoreo del espectro electromagnético, la cual, según la Ley 1621/13, debe distinguirse de la interceptación de comunicaciones personales, y en ese sentido su realización no requiere de control judicial. La información recogida a través de este método no que no sirva para los propósitos de inteligencia no podrá ser almacenada y deberá ser destruida (Ley 1621/13, artículo 17).

El segundo método es requerir a los operadores de servicios de telecomunicaciones información que ayude a la identificación y localización de los usuarios de estos servicios.

iv. **Procedimiento para la realización de estas actividades:** la legislación consagra un procedimiento estándar para la autorización de las actividades de inteligencia y contrainteligencia. Deben ser autorizadas por el director de la dependencia encargada de iniciar tareas de inteligencia y deberá incluir un planeamiento. Igualmente, se prevé que el nivel de autorización requerido para cada operación o misión de trabajo se incremente en consideración a la naturaleza y posible impacto de la actividad, al tipo de objetivo, al nivel de riesgo para las fuentes o los agentes, y a la posible limitación de derechos fundamentales (Ley 1621, artículo 14). Al emitir las autorizaciones de operaciones de inteligencia, el superior jerárquico que lo haga deberá revisar que efectivamente se relacionen con los fines legales de las actividades de inteligencia y se ajuste a los límites previstos en la ley, según se encuentran definidos en los artículos 4 y 5 de la Ley 1621/13 (Ley 1621/13, artículo 15).

v. **Controles que pueden ejercerse:** la legislación colombiana prevé un control político para las actividades de inteligencia, a cargo de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia. Las funciones principales de esta comisión son las siguientes: hacer control y seguimiento político, verificar el uso eficiente de los recursos y comprobar la legalidad de las actuaciones de los servicios de inteligencia.

También resultan aplicables controles disciplinarios internos. Por ejemplo, se establece que los superiores jerárquicos de las entidades que ejercen funciones de inteligencia serán responsables disciplinariamente por las órdenes de operaciones o las misiones de trabajo que autoricen, sin que puedan alegar obediencia debida para eximirse de responsabilidad (Ley 1621/13, artículo 15).

c. Vigilancia de las comunicaciones en el marco de investigaciones penales

Las facultades de las autoridades encargadas de la investigación penal que pueden afectar la confidencialidad de las comunicaciones se encuentran previstas en la Ley 906 de 2004, en la cual se encuentra el Código de Procedimiento Penal.

i. **Facultades de las autoridades de investigación que interfieren con las comunicaciones personales:** la legislación procesal penal colombiana contempla tres procedimientos que son especialmente relevantes en materia de vigilancia de las comunicaciones personales. En primer lugar, faculta la interceptación, mediante grabación magnetofónica o similares, de "las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación" (Ley 906 de 2004, artículo 235).

   Segundo, también habilita la aprehensión de los equipos y medios de almacenamiento que pudieran haber sido utilizados por el investigado para transmitir información útil para la investigación que se adelante a través de internet u otros medios tecnológicos que produzcan efectos equivalentes (Ley 906, artículo 236).

   Tercero, permite la retención de correspondencia "privada, postal, telegráfica o de mensajería especializada o similar" (Ley 906, artículo 233).

ii. **Autoridades que pueden ordenar la vigilancia:** compete a la Fiscalía General de la Nación ordenar las tres facultades antes mencionadas (Ley 906, artículo 114), las cuales serán llevadas a cabo por la policía judicial.

iii. **Circunstancias en las que tales facultades pueden ejercerse:** la interceptación de comunicaciones puede ordenarse con el único objeto de buscar elementos materiales probatorios y evidencia física (Ley 906, artículo 235). Se excluye la interceptación de comunicaciones entre el procesado y su defensor (Ley 906, artículo 235).

   Por su parte, la recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes podrá ordenarse cuando el fiscal del proceso tenga motivos razonables para inferir, de acuerdo con los medios cognoscitivos previstos en la Ley 906 de 2004, que el indiciado o imputado está haciendo uso de ellos para transferir información útil para la investigación que se adelanta (Ley 906, artículo 236).

   De forma similar, la retención de correspondencia procede cuando el fiscal del proceso tenga motivos razonables para inferir, de acuerdo con los medios cognoscitivos previstos en la Ley 906 de 2004, que ella contiene información útil para la investigación que se adelanta (Ley 906, artículo 233).

iv. **Procedimiento que debe seguirse para que se ordene una actuación de vigilancia de comunicaciones:** corresponde a la Fiscalía General de la Nación ordenar la práctica de interceptación de comunicaciones, de recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes y de retención de correspondencia (Ley 906, artículos 114, 233, 235 y 236).

En el caso de la interceptación de comunicaciones, la orden deberá fundamentarla por escrito. Tendrá una vigencia máxima de 3 meses, prorrogable hasta por el mismo tiempo si subsisten los motivos fundados que le dieron origen. Quienes participen en la realización de la interceptación de comunicaciones tienen el deber de guardar reserva sobre ellas (Ley 906, artículo 235).

Con relación a la retención de correspondencia, podrá solicitarse a las oficinas correspondientes y a las empresas de mensajería especializada los mensajes transmitidos o recibidos por el investigado, así como la relación de envíos hechos por su solicitud o dirigidos a él. Se indica a su vez que la retención de correspondencia no podrá prolongarse por más de un año (Ley 906, artículo 233).

Con relación a la recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes, se indica que la aprehensión se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida e inmediatamente después se devolverán los equipos incautados (Ley 906, artículo 236).

Por su parte, tanto en el caso de la retención de correspondencia como en el de recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes el procedimiento aplicable es similar al previsto para registros y allanamientos. En ese sentido, entre otras, debe determinarse con precisión, si fuera posible, los lugares donde se encuentran los equipos o las comunicaciones que se van a retener, así como los equipos cuyos datos se van a determinar (Ley 906, artículo 222).

v. **Controles aplicables a la vigilancia de las comunicaciones en materia penal:** el control judicial a las medidas mencionadas en este acápite es posterior, dentro de las 24 horas siguientes al diligenciamiento de las órdenes correspondientes. El control se realizará en audiencia, a la que acudirán el fiscal, los miembros de la policía judicial y, de ser el caso, los peritos que intervinieron en la práctica de las medidas. A su vez, dependiendo de la etapa en la que se encuentre el proceso penal, podrán acudir el procesado y su defensor. El juez de control de garantías podrá interrogar a los comparecientes y deberá decidir de inmediato sobre la validez del procedimiento (Ley 906, artículo 237). Esta decisión no podrá ser impugnada, aunque la defensa podrá controvertirla posteriormente en caso de no haber participado en la audiencia de legalización de las medidas (Ley 906, artículo 238).

México

a. Marco constitucional de la vigilancia de las comunicaciones

La Constitución Política de los Estados Unidos Mexicanos establece el derecho a la inviolabilidad de las comunicaciones y regula un amplio catálogo de garantías relacionadas con este derecho. Entre las más destacables se encuentran las siguientes: el deber de sancionar el desconocimiento de la libertad o secreto de las comunicaciones; la reserva judicial para la intercepción de cualquier comunicación privada, indicando que debe ser autorizada por una autoridad judicial federal, a petición de la autoridad federal que señale la ley o del titular del Ministerio Público de una entidad federativa; el deber de la autoridad federal correspondiente de motivar la solicitud y de identificar con precisión la persona afectada, la duración y los medios; y algunos tipos de asuntos sobre los cuales no podrá proceder la intervención de comunicaciones (a saber: cuestiones de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni las comunicaciones del detenido con su defensor) (artículo 16, párrafos 12 y 13).

Adicionalmente, al señalar que el servicio de telecomunicaciones es un servicio público, la Constitución indica que el Estado deberá garantizar que sea prestado bajo ciertas condiciones, incluyendo la ausencia de injerencias arbitrarias (artículo 6, literal B, numeral II).

En relación con el valor jurídico de los tratados internacionales en materia de derechos humanos, a partir de una reforma constitucional introducida en 2011, el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos establece que todas las personas en México gozan de los derechos reconocidos en la Constitución y en los tratados internacionales en los que el Estado mexicano sea parte. A su vez, se afirma también que "[l]as normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia".

b. Vigilancia de las comunicaciones en el marco de actividades de inteligencia y contrainteligencia

La Ley de Seguridad Nacional establece el marco jurídico de las actividades de inteligencia en México.

i. **Autoridades que pueden realizar labores de inteligencia y contrainteligencia:** el Consejo de Seguridad Nacional es el responsable de establecer y articular la política en esta materia. Está compuesto por distintos servidores públicos, incluyendo distintos secretarios del Gobierno federal y el Procurador General de la Nación (Ley de Seguridad Nacional, artículo 12). Entre sus funciones se encuentra definir "los lineamientos para regular el uso de aparatos útiles en la intervención de comunicaciones privadas" (Ley de Seguridad Nacional, artículo 13).

   Por otra parte, el Centro Nacional de Inteligencia es el órgano al que le corresponde operar las tareas de inteligencia, como parte del sistema de seguridad nacional.

ii. **Definición y límites de las labores de inteligencia:** la inteligencia se define como "el conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de información, para la toma de decisiones en materia de Seguridad Nacional. A su vez, la legislación mexicana tiene una amplia definición de seguridad nacional, al enlistar una serie de finalidades que se entiende que hacen parte de este concepto. También se incluye un amplio listado de actividades que se consideran amenazas a la seguridad nacional. Tal listado, previsto en el artículo 5 de la Ley de Seguridad Nacional, es importante porque la norma que se refiere la intervención de comunicaciones en materia de inteligencia hace referencia a él para determinar las circunstancias en las que procede (Ley de Seguridad Nacional, artículo 35). Dispone dicho artículo lo siguiente:

> *Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:*
> *I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;*
> *II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;*
> *III. Actos que impidan a las autoridades actuar contra la delincuencia organizada;*
> *IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;*
> *V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;*
> *VI. Actos en contra de la seguridad de la aviación;*
> *VII. Actos que atenten en contra del personal diplomático;*
> *VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;*
> *IX. Actos ilícitos en contra de la navegación marítima;*
> *X. Todo acto de financiamiento de acciones y organizaciones terroristas;*
> *XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia;*
> *XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos, y*
> *XIII. Actos ilícitos en contra del fisco federal a los que hace referencia el artículo 167 del Código Nacional de Procedimientos Penales.*

A su vez, se definen las tareas de contrainteligencia como "las medidas de protección de las instancias en contra de actos lesivos, así como las acciones orientadas a disuadir o contrarrestar su comisión" (Ley de Seguridad Nacional, artículo 32).

Por su parte, en cuanto a los límites, se indica que, al utilizar cualquier método de recolección de información, las autoridades de inteligencia deben respetar las garantías individuales y los derechos humanos (Ley de Seguridad nacional, artículo 31).

iii. **Facultades que tienen estas autoridades que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones:** la Ley se Seguridad Nacional señala que "las instancias [de inteligencia] gozarán de autonomía técnica y podrán hacer uso de cualquier método de recolección de información" (Ley de Seguridad Nacional, artículo 31).

Además de esta disposición general, dicha ley en todo caso hace referencia a una facultad específica que permite la recolección de información de inteligencia y que limita la confidencialidad de la información. Se trata de la intervención de comunicaciones privadas, la cual podrá ser solicitada por el Centro Nacional de Inteligencia en los casos identificados por el artículo 5 de la Ley de Seguridad Nacional como amenazas a la seguridad nacional (Ley de Seguridad Nacional, artículo 34). Tal intervención resulta aplicable a "comunicaciones y emisiones privadas, realizadas por cualquier medio de transmisión, conocido o por conocerse, o entre presentes, incluyendo la grabación de imágenes privadas" (Ley de Seguridad Nacional, artículo 39).

iv. **Procedimiento para la realización de estas actividades:** el único procedimiento de inteligencia que se encuentra regulado con precisión es el relacionado con la intervención de comunicaciones privadas. En este sentido, se señala que el Centro Nacional de Inteligencia podrá solicitar autorización judicial para la realización de intervenciones de comunicaciones por cuestiones de seguridad nacional (Ley de Seguridad Nacional, artículo 34). Solo podrá autorizarse en presencia de una de las amenazas a la seguridad nacional definidas en el artículo 5 de la Ley de Seguridad Nacional. La solicitud deberá contener una descripción detallada de las supuestas amenazas para la seguridad nacional, las consideraciones que motivan la solicitud y el tiempo de vigencia de la autorización que se solicita (Ley de Seguridad Nacional, artículo 38). El juez deberá resolverla dentro de las 24 horas siguientes a recibirla. En caso de autorizarla, deberá indicar con precisión los datos de la persona cuyas comunicaciones se permite intervenir, así como la duración de la medida. En caso de negarla, deberá fundamentar su decisión y mencionar los requisitos que, de subsanarse, la harían procedente (Ley de Seguridad Nacional, artículo 39). Las autorizaciones se conceden por un plazo máximo de 180 días, prorrogables por el mismo lapso (Ley de Seguridad Nacional, artículo 43).

v. **Controles que pueden ejercerse:** la intervención de comunicaciones por razones de inteligencia requiere de autorización judicial. Los juzgados que conocen de las solicitudes de intervención de comunicaciones en materia de Seguridad Nacional serán determinados por el Poder Judicial de la Federación (Ley de Seguridad Nacional, artículo 35). El juez que la haya autorizado podrá solicitar informes periódicos sobre su ejecución (Ley de Seguridad Nacional, artículo 41). El control judicial previo también es necesario incluso en los casos de urgencia, aunque en esta hipótesis el juez podrá autorizar de inmediato la medida que se requiera (Ley de Seguridad Nacional, artículo 49).

Adicionalmente, existe un control interno relacionado con el mantenimiento de la confidencialidad de toda la información de inteligencia, incluyendo la conseguida a través de intervención de comunicaciones. En este sentido, el Centro Nacional de Inteligencia debe adoptar medidas de seguridad de la información con motivo de los sistemas de coordinación en materia de seguridad nacional (Ley de Seguridad Nacional, artículo 55).

Finalmente, la legislación mexicana establece una Comisión Bicameral en el Poder Legislativo Federal para el control y evaluación de las políticas y acciones en materia de seguridad nacional. Dentro de sus funciones no se encuentra la de requerir información específica sobre el cumplimiento de sus funciones, pero sí la de revisar los resultados de las revisiones, auditorías y procedimientos que se practiquen al Centro Nacional de Inteligencia (Ley de Seguridad Nacional, artículo 57).

c. Vigilancia de las comunicaciones en el marco de investigaciones penales

En México, el marco legal de las facultades que interfieren con la confidencialidad de las comunicaciones personales en el marco de un proceso penal es complejo. Este se encuentra previsto, de forma general, en el Código Nacional de Procedimientos Penales (en adelante, "CNPP"), publicado el 5 de marzo de 2014. Otras disposiciones contenidas en leyes que regulan aspectos penales específicos reiteran esta facultad. Así sucede, por ejemplo, con la Ley general para prevenir y sancionar los delitos en materia de secuestro (artículo 24) y la Ley federal contra la delincuencia organizada (artículos 8 y 16 a 28).

Adicionalmente, conviene mencionar que a la Guardia Nacional se le confiere la función de prevenir el crimen, y en el ejercicio de ella puede hacer uso de ciertas facultades que implican la limitación de la confidencialidad de las comunicaciones (Ley de la Guardia Nacional).

i. **Facultades de las autoridades de investigación que interfieren con las comunicaciones personales:** la legislación mexicana faculta la intervención de comunicaciones privadas en el marco de procedimientos penales. Así, el artículo 291 del CNPP dispone lo siguiente:

> *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.*

El artículo 294 del CNPP establece un límite a la intervención de comunicaciones, disponiendo que no procederá en materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de comunicaciones entre un detenido con su defensor. De esta forma, se repite la regla de exclusión prevista en el párrafo 13 del artículo 16 de la Constitución.

Otra facultad que en el marco de los procedimientos penales puede restringir la privacidad de las comunicaciones personales es la geolocalización y la solicitud de entrega de datos conservados.

ii. **Autoridades que pueden ordenar la vigilancia:** la intervención de comunicaciones privadas puede ser solicitada tanto por el titular de la Procuraduría General de la República, como por los procuradores de las 32 entidades federativas. Deberá ser resuelta por el juez federal de control competente (CNPP, artículo 291).

También, se confiere a la Guardia Nacional la facultad de solicitar, a través del comandante o del titular de la jefatura policial de Coordinación Militar Policial, autorización judicial para la intervención de comunicaciones (Ley de la Guardia Nacional, artículo 100). Conviene mencionar que la Guardia Nacional es un órgano de la Secretaría de Seguridad y Protección Ciudadana, al que le corresponde la función, entre otras, de prevenir la comisión de delitos (Ley de la Guardia nacional, artículo 7, numeral II), y es en ejercicio de esta función que se le asignan ciertas facultades que interfieren con la confidencialidad de las comunicaciones personales.

Igualmente, el Procurador, o el servidor público en quien se delegue tal competencia, podrá solicitar al juez que ordene a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos la entrega de información que permita la geolocalización de la persona investigada. Igualmente, podrá solicitar la entrega de datos conservados por tales concesionarios. Tal deber de conservación o retención de datos está regulado por la propia ley penal y se refiere a la "a conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días" (CNPP, artículo 303). Tal atribución también se le asigna, en el marco de la prevención de delitos, a la Guardia Nacional, previa autorización judicial (Ley de la Guardia Nacional, artículo 9, numeral XXVI).

iii. **Circunstancias en las que tales facultades pueden ejercerse:** la legislación mexicana no especifica las circunstancias en las que procede la interceptación de comunicaciones en el marco de una investigación penal. Así, la falta de precisión sobre este asunto contrasta con la especificidad con la que se regulan otros temas, como por ejemplo el tipo de comunicaciones sobre los que procede la interceptación.

En cambio, la ley sí regula con mayor detalle la intervención de comunicaciones personales que puede solicitar la Guardia Nacional, al indicar que esta procede solo "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 (Ley de la Guardia Nacional)" (Ley de la Guardia Nacional, artículo 100).

Adicionalmente, la legislación mexicana tampoco especifica las circunstancias en las que procede la solicitud de entrega de datos conducente a la geolocalización del investigado o de los datos conservados; únicamente se especifican los supuestos en los que tal solicitud procede sin control judicial previo (CNPP, artículo 303).

iv. **Procedimiento que debe seguirse para que se ordene una actuación de vigilancia de comunicaciones:** en la solicitud de intervención de las comunicaciones debe ser motivada, indicando la necesidad de su práctica y especificando la siguiente información: "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" (CNPP, artículo 292).

El juez federal de control competente deberá resolverla máximo dentro de las 6 horas siguientes a recibirla (CNPP, artículo 291). En su decisión, indicará las características de la intervención, sus modalidades y límites. Igualmente, de ser el caso, indicará a las instituciones públicas o privadas los modos específicos de colaboración (CNPP, artículo 293).

La legislación mexicana establece un deber de los titulares de medios o sistemas susceptibles de intervención para que colaboren con la autoridad competente para operar una orden de intervención de comunicaciones privadas. A su vez, se indica que el incumplimiento de este mandato dará lugar a las sanciones penales que resulten aplicables (CNPP, artículo 301).

En cuanto a la entrega de datos conducentes para la geolocalización o los conservados por los concesionarios, se especifica el contenido de la solicitud, la cual deberá incluir, entre otros, los equipos de comunicación móvil relacionados con los hechos que se investigan, los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados y su duración. La petición deberá ser resuelta de manera inmediata. En determinadas circunstancias, el Fiscal General de la República, o el servidor público en quien se delegue tal facultad, podrá ordenar la entrega de esta información directamente a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos. Ello podrá suceder en los siguientes casos: "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". Una vez cumplido el requerimiento, deberá informarse al juez de control dentro de las 48 horas siguientes para que ratifique de forma parcial o total la subsistencia de la medida. Si no la ratifica, la información obtenida no podrá ser incorporada al proceso penal (CNPP, artículo 303).

v. **Controles aplicables a la vigilancia de las comunicaciones en materia penal:** en relación con la intervención de comunicaciones privadas, el juez decidirá si la autoriza (CNPP, artículo 291). Asimismo, podrá en cualquier momento verificar que sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocatoria parcial o total (CNPP, artículo 294). Por otro lado, una vez concluida la diligencia, la Fiscalía General de la República informará al juez (CNPP, artículo 299). Este podrá ordenar la destrucción de los registros de intervención de comunicaciones privadas que no se relacionen con los delitos investigados ni con otros delitos que hayan ameritado la apertura de una investigación, salvo que la defensa solicite que sean preservados (CNPP, artículo 300).

   En cuanto a la entrega de información para geolocalización y la entrega de datos conservador, existe control judicial previo por parte del juez de control competente. No obstante, en determinadas circunstancias, la medida puede ser ordenada directamente por el Fiscal General de la República o quien sea delegado para este efecto, caso en el cual el control judicial será posterior (CNPP, artículo 303).

Panamá

a. Marco constitucional de la vigilancia de las comunicaciones

La Constitución Política de la República de Panamá establece dos reglas relacionadas con la privacidad de las comunicaciones. Así, el primer párrafo del artículo 29 establece que la correspondencia y los demás documentos privados son inviolables, por lo que no pueden ser examinados ni retenidos, sino mediante orden de autoridad competente y para fines concretos, en cumplimiento de las formas que prevea la ley. Agrega además esta disposición que debe guardarse absoluta reserva con relación a los asuntos ajenos al objeto del examen o retención.

Por su parte, el inciso tercero del mismo artículo establece el derecho a la inviolabilidad de las comunicaciones privadas, disponiendo que no podrán ser interceptadas o grabadas sino mediando mandato de autoridad judicial. Como consecuencia de lo anterior, se dispone que no podrán usarse como prueba la información recolectada en incumplimiento de las formalidades indicadas.

Finalmente, la Constitución de Panamá no contiene una cláusula específica que haga referencia al valor normativo de los tratados internacionales sobre derechos humanos.

b. Vigilancia de las comunicaciones en el marco de actividades de inteligencia y contrainteligencia

A diferencia de los demás países incluidos en este documento, Panamá no tiene una ley que de forma general regule los servicios de inteligencia en ese país, sino una serie de normas que regulan de forma separada las facultades de distintos organismos que ejercen tareas de inteligencia. Dentro de las distintas normas que se ocupan de esto, se destaca el Decreto Ejecutivo 263 de 2010, que creó el Consejo de Seguridad Nacional.

Autoridades que pueden realizar labores de inteligencia y contrainteligencia: el Consejo de Seguridad Nacional, integrado por el presidente de la República y el Ministro de la Presidencia (Decreto Ejecutivo 263 de 2010, artículo 3), estará encargado de fijar los objetivos anuales de inteligencia (Decreto Ejecutivo 263 de 2010, artículo 5). Este órgano tendrá una Secretaría Ejecutiva, a la que le compete, entre otras, realizar tareas de inteligencia que contribuyan a preservar la integridad, estabilidad y permanencia de la República de Panamá, manteniendo la gobernabilidad y el Estado de derecho" (Decreto Ejecutivo 263 de 2010, artículo 15).

Definición y límites de las labores de inteligencia: no existe una definición legal específica de las funciones de inteligencia.

En cuanto a los límites, se establece que la Secretaría Ejecutiva del Consejo de Seguridad Nacional debe realizar todas sus actuaciones, incluidas las de inteligencia, con "respeto a los derechos humanos y a las garantías fundamentales, y [en] estricto cumplimiento de la Constitución, la ley, y los tratados y convenios internacionales ratificados por la República de Panamá" (Decreto Ejecutivo 263 de 2010, artículo 11). Adicionalmente, se prohíbe a la Secretaría Ejecutiva vulnerar los derechos consagrados en la Constitución y en las leyes; la participación en cualquier actividad política partidista; difundir cualquier información que hubiera conocido debido a sus actividades; cualquier otra actividad que atente contra la integridad física y moral,

honra y bienes de los asociados; y la realización de actividades que involucren espionaje político (Decreto Ejecutivo 263 de 2010, artículo 13).

Facultades que tienen estas autoridades que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones: la Secretaría Ejecutiva del Consejo de Seguridad podrá solicitar a las personas naturales o jurídicas los datos, estadísticas e informaciones que estén relacionadas con la seguridad nacional, así como a prestar apoyo y colaboración necesaria, salvo en los casos en los que se requiera autorización judicial.

Adicionalmente, se establece un deber de crear y conservar un registro de datos de identificación y dirección suministradas por las personas naturale o jurídicas a cargo de las empresas concesionarias, los distribuidores, los agentes autorizados y los revendedores de telefonía móvil, fija y troncal, los café-Internet, los info-plazas y las redes de comunicación (Decreto Ejecutivo 263 de 2010, artículo 21).

Procedimiento para la realización de estas actividades: no se establece un procedimiento detallado para la realización de labores de inteligencia.

Controles que pueden ejercerse: no se especifican los controles que proceden con relación a las actividades de inteligencia.

c. Vigilancia de las comunicaciones en el marco de investigaciones penales

Las facultades de investigación que interfieren con la inviolabilidad de las comunicaciones se encuentran reguladas en el Código de Procedimiento Penal

Facultades de las autoridades de investigación que interfieren con las comunicaciones personales: la legislación procesal penal panameña prevé dos medidas de investigación que interfieren con la inviolabilidad de las comunicaciones. Se trata de la incautación de correspondencia y la "grabación de conversaciones e interceptación de comunicaciones cibernéticas, seguimientos satelitales, vigilancia electrónica y comunicaciones telefónicas" (Código Procesal Penal, artículos 310 y 311).

Autoridades que pueden ordenar la vigilancia: corresponde al fiscal solicitar la autorización de estas medidas, lo cual será decidido por el juez de control de garantías (Código Procesal Penal, artículos 310 y 311).

Circunstancias en las que tales facultades pueden ejercerse: las normas penales que regulan estas facultades indican que ellas proceden para acreditar la existencia de un hecho punible y la vinculación de determinada persona en su comisión. También se establece que la intervención de comunicaciones es excepcional (Código Procesal Penal, artículo 311).

Procedimiento que debe seguirse para que se ordene una actuación de vigilancia de comunicaciones: el fiscal es el encargado de solicitar la grabación de conversaciones y la interceptación de comunicaciones, lo cual debe ser resuelto por el juez de control de garantías. En caso de concederla, la medida no podrá otorgarse por más de 20 días, prorrogables a petición del fiscal, quien deberá justificar su solicitud. Debe guardarse la confidencialidad de las comunicaciones, por lo que los funcionarios que participaron en la interceptación deben guardar secreto sobre

ellas y lo recaudado debe guardarse en una cadena de custodia (Código Procesal Penal, artículo 311).

Controles aplicables a la vigilancia de las comunicaciones en materia penal: el juez de control de garantías debe conceder la realización de las medidas de investigación previstas en los artículos 310 y 311 del Código Procesal Penal.

Paraguay

a. Marco constitucional de la vigilancia de las comunicaciones

La Constitución de la República de Paraguay de 1992 establece la inviolabilidad de las comunicaciones privadas. Así, el artículo 36 establece una lista de documentos y actividades a las que se les confiere el carácter de inviolables, dentro de los que se incluyen "las comunicaciones telefónicas, telegráficas, cablegráficas o de cualquier otra especie". Se añade que, como consecuencia de lo anterior, tales comunicaciones no pueden ser examinadas, reproducidas, interceptadas o secuestradas, excepto en el caso de que exista orden judicial, de que se trate de cuestiones específicas previstas en la ley y que se trate de información indispensable para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades.

Respecto del valor jurídico de los tratados internacionales en materia de derechos humanos, la Constitución le otorga a los tratados, convenios y acuerdos internacionales en general un valor inferior a ella, pero superior al de las leyes (Constitución de la República de Paraguay, artículo 137).

La ley suprema de la República es la Constitución. Esta, los tratados, convenios y acuerdos internacionales aprobados y ratificados, las leyes dictadas por el Congreso y otras disposiciones jurídicas de inferior jerarquía, sancionadas en su consecuencia, integran el derecho positivo nacional en el orden de prelación enunciado.

b. Vigilancia de las comunicaciones en el marco de actividades de inteligencia y contrainteligencia

i. **Autoridades que pueden realizar labores de inteligencia y contrainteligencia:** los distintos organismos que cumplen funciones de inteligencia componen el Sistema Nacional de Inteligencia, con el propósito de actuar de manera coordinada y articulada para producir conocimiento útil con el propósito de lograr la paz y la seguridad del Estado, proteger la soberanía nacional, presentar el orden constitucional y el régimen democrático vigente (Ley 5.241, artículo 7). Tales órganos son los siguientes: el Consejo Nacional de Inteligencia, el Ministerio del Interior, el Ministerio de Defensa Nacional, las Fuerzas Armadas de la Nación, la Secretaría Permanente del Consejo de Defensa Nacional, la Secretaría Nacional Antidrogas y la Secretaría e Prevención de Lavado de Dinero o Bienes (Ley 5.241, artículo 10).

   La Secretaría Nacional de Inteligencia es el órgano especializado encargado de realizar labores de inteligencia y analizar la información recolectada para comunicar a las autoridades sobre los eventuales riesgos y amenazas a determinados fines del Estado (Ley 5.241, artículo 14).

ii. **Definición y límites de las labores de inteligencia:** la legislación paraguaya define la inteligencia como el "conocimiento útil, resultado del procesamiento sistemático de recolección, evaluación y análisis de información, desarrollado por un organismo profesional, para asesorar en sus decisiones a los niveles de conducción superior del Estado identificados en la presente Ley, en lo relativo con el logro de los objetivos nacionales, para garantizar la paz, la seguridad y la defensa nacional. Dicho conocimiento estará destinado a prevenir, advertir e informar de cualquier amenaza o riesgo que afecten los intereses nacionales" (Ley 5.241, artículo 2).

Por su parte, contrainteligencia es definida como la parte de las labores de inteligencia destinadas a identificar acciones de inteligencia desarrolladas por Estados o grupos extranjeros, que puedan afectar la paz, la seguridad, las autoridades, la defensa nacional o el régimen democrático (Ley 5.241, artículo 2).

Adicionalmente, se identifican "7(siete) principios fundamentales que orientan las actividades del Sistema Nacional de Inteligencia". Algunos de ellos son características específicas del diseño del sistema de inteligencia en Paraguay, mientras que otros se refieren a límites sustantivos que deben ser tenidos en cuenta en todo momento en la realización de las actividades de inteligencia. Se trata de los siguientes: respeto al ordenamiento jurídico, respeto al régimen democrático, respecto de los derechos constitucionales, autorización judicial previa, proporcionalidad, reserva y utilización exclusiva de la información (Ley 5.241, artículo 3).

Complementan estos principios una serie de prohibiciones que deben tenerse en cuenta al definir el propósito de las actividades de inteligencia. Así, se establece que estas no pueden ejercerse con propósitos discriminatorios, ni para influir en la situación institucional, política, militar, policial, social o económica del país, ni para realizar labores represivas, de policía o de investigación criminal, ni para revelar o divulgar información obtenida en el marco de sus actividades (Ley 5.241, artículo 5).

iii. **Facultades que tienen estas autoridades que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones:** las autoridades que realizan labores de inteligencia tienen la facultad de utilizar métodos para recolectar información privada cuando existan "fundadas sospechas de amenaza grave para la seguridad colectiva de las personas, autoridades o instituciones, o de la seguridad pública o del Estado de derecho" (Ley 5.241, artículo 3).

Además, se establecen los siguientes procedimientos específicos de obtención de información: intervención de comunicaciones telefónicas, informáticas, radiales y de correspondencia en cualquiera de sus formas; la intervención de sistemas y redes informáticas; la escucha y grabación electrónica audiovisual; y la intervención de cualquier otro sistema tecnológico destinado a la transmisión, almacenamiento o procesamiento de comunicaciones o información (Ley 5.241, artículo 25).

Estos procedimientos podrán ejercerse cuando la información que se busca no pueda obtenerse por fuentes abiertas y deben limitarse a la obtención de información indispensable para el cumplimiento de ciertos fines: resguardar la paz y la seguridad nacional, la estabilidad institucional, la protección frente a amenazas de terrorismo, crimen organizado y narcotráfico, así como para la defensa del régimen democrático (Ley 5.241, artículo 24).

iv. **Procedimiento para la realización de estas actividades:** para poder realizar los procedimientos especiales de obtención de información, el Secretario Nacional de Inteligencia deberá solicitarlos. En caso de ser autorizada por el juez de control de garantías, en la resolución que así se decida deberá especificarse los medios que se emplearán, las personas a quienes se aplicará y la duración de la medida, que tendrá un límite de 90 días, prorrogables por otro tanto por una sola vez (Ley 5.241, artículo 26).

v. **Controles que pueden ejercerse:** uno de los llamados 7 principios fundamentales que orientan las actividades del Sistema Nacional de Inteligencia es el de control judicial previo, de acuerdo con el cual toda actuación de dicho sistema para la obtención de información personal requiere autorización judicial previa (Ley 5.241, artículo 3). La autorización de tales procedimientos debe realizarse ante un juez de control de garantías, quien deberá decidir dentro de las 24 horas siguientes a su presentación (Ley 5.241, artículo 26).

c. Vigilancia de las comunicaciones en el marco de investigaciones penales

Las facultades de investigación en el marco de procesos penales que pueden interferir con la inviolabilidad de las comunicaciones personales se encuentran reguladas en Paraguay por la Ley 1.286, que establece el Código Procesal Penal. Adicionalmente, la Ley 1.881, relacionada con la investigación de delitos de tráfico ilícito de estupefacientes, contiene algunas regulaciones especiales en materia de interceptación de comunicaciones cuando se trata de esos delitos.

i. **Facultades de las autoridades de investigación que interfieren con las comunicaciones personales:** se podrá ordenar la intercepción y secuestro de correspondencia (Ley 1.286, artículo 198), así como la intervención de las comunicaciones del acusado, cualquiera fuera el medio técnico empleado (Ley 1.286, artículo 200).

   Es importante mencionar que el artículo 316 de la Ley 1.286 establece que el Ministerio Público puede exigir directamente (es decir, sin que se necesite autorización judicial) información sobre cualquier funcionario o empleado público y que todas las autoridades están obligadas a colaborar con la investigación y a atender pedidos de información, lo cual ha sido entendido en el sentido de habilitar a esta entidad a solicitar metadatos de llamadas telefónicas sin autorización judicial.[6]

ii. **Autoridades que pueden ordenar la vigilancia:** corresponde al juez ordenar la realización de medidas de investigación como la interceptación de comunicaciones (Ley 1.286, artículos 198 y 200), a solicitud de la Fiscalía (Ley 1.286, artículo 52).

   En el caso de la investigación de delitos relacionados con tráfico ilícito de estupefacientes, quienes se encuentran facultados para solicitar la interceptación de comunicaciones son la Secretaría Nacional Antidroga o la Fiscalía, lo cual deberá ser resuelto por un juez (Ley 1.881, artículo 88).

iii. **Circunstancias en las que tales facultades pueden ejercerse:** la legislación paraguaya prevé que podrá realizarse la interceptación y secuestro de correspondencia "siempre que sea útil para la investigación de la verdad" (Ley 1.286, artículo 198). Por su parte, no hay una referencia específica sobre la procedencia de la intervención de comunicaciones en la legislación procesal general (Ley 1.286, artículo 200).

6 Corte Suprema de Justicia. Sala Penal: Materia Penal. Inviolabilidad De La Comunicación Privada. Pruebas. Medios De Prueba. Prueba De Peritos. Cruce De Llamadas. Acuerdo y Sentencia N° 711 del 20/08/14.

iv. **Procedimiento que debe seguirse para que se ordene una actuación de vigilancia de comunicaciones:** los resultados de la intervención de comunicaciones solo podrán ser entregados al juez que la haya ordenado, quien deberá decidir sobre si guarda relación con el hecho que se investiga, caso en el cual decidirá conservar la información. También deberá decidir la destrucción de la totalidad o de las partes de la información que no tengan tal relación (Ley 1.286, artículo 200).

   De forma similar, tratándose de interceptación y secuestro de correspondencia, será el juez quien leerá su contenido y determinará si la conserva, dependiendo de la relación que existe con el hecho investigado (Ley 1.286, artículo 198).

   Por su parte, con relación a los delitos de tráfico ilícito de estupefacientes, la regulación es más detallada en cuanto al procedimiento a seguir para la realización de interceptación de comunicaciones. Así, se indica que la solicitud que se formule para la realización de esa medida deberá indicarse el tipo de comunicaciones que se propone interceptar, registrar, grabar o reproducir, los medios técnicos que se emplearán para ese propósito y los logros que se espera obtener mediante el uso de tales medidas. Se señala también que el juez podrá exigir al solicitante elementos de juicio adicionales. En la realización de los procedimientos, se transcribirán en acta o se conservarán solo los documentos recolectados relacionados con los hechos investigados (Ley 1.881, artículo 88).

v. **Controles aplicables a la vigilancia de las comunicaciones en materia penal:** existe control judicial previo de las medidas restrictivas de la inviolabilidad de las comunicaciones (Ley 1.286, artículos 198 y 200).

Perú

a. Marco constitucional de la vigilancia de las comunicaciones

El numeral 10 del artículo 2 de la Constitución Política del Perú regula el derecho a la inviolabilidad de las comunicaciones y establece sus garantías. De esta forma, señala que las "Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley". Asimismo, se establece una regla que limita la excepción al derecho a la inviolabilidad de las comunicaciones a aquellos asuntos que motivaron su examen. También se excluye valor probatorio a los documentos que no hubieran sido obtenidos en cumplimiento de lo previsto en este artículo.

En cuanto al valor jurídico de los tratados internacionales en materia de derechos humanos, la Constitución no contiene una cláusula específica; en cambio, señala de forma general que los tratados tienen rango de ley (artículo 200, párrafo 4).

b. Vigilancia de las comunicaciones en el marco de actividades de inteligencia y contrainteligencia

Dos leyes son de particular importancia para el marco normativo de las actividades de inteligencia en Perú. Se trata de la Ley 27.479, que regula el Sistema de Inteligencia Nacional, y la Ley 28.664, que también regula el Sistema de Inteligencia Nacional y además se ocupa de la Dirección Nacional de Inteligencia.

i. **Autoridades que pueden realizar labores de inteligencia y contrainteligencia:** el conjunto de órganos del Estado que realizan funciones de inteligencia se agrupa bajo el Sistema de Inteligencia Nacional, con el propósito de actuar de forma coordinada en el desempeño de esta función (Ley 28.664, artículo 5). Se encuentra integrado por organismos de los sectores de defensa, interior y relaciones exteriores, además del Consejo de Inteligencia Nacional y de la Dirección Nacional de Inteligencia (Ley 28.664, artículos 6 a 11).

   Esta última es el organismo especializado que tiene a su cargo la producción de la inteligencia y la ejecución de las medidas de contrainteligencia, en ámbitos distintos a la inteligencia militar (Ley 28.664, artículos 8 y 23).

ii. **Definición y límites de las labores de inteligencia:** según la definición legal, las actividades de inteligencia tienen el propósito de proporcionar al Presidente de la República y al Consejo de Ministros de "conocimiento útil, obtenido mediante el procesamiento de las informaciones, sobre las amenazas y riesgos actuales y potenciales, que puedan afectar la seguridad nacional y el ordenamiento constitucional de la República" (Ley 28.664, artículo 3).

   A su vez, se establecen una serie de principios que deben guiar el funcionamiento de estas actividades, a saber: legalidad, legitimidad, control democrático, pertinencia, circulación restringida, especialidad y planificación (Ley 28.664, artículo 4). Mas que límites sustantivos, se trata de principios operativos para el adecuado funcionamiento de los servicios de inteligencia.

iii. **Facultades que tienen estas autoridades que pueden interferir con los derechos a la intimidad y al secreto de las comunicaciones:** con el propósito de recolectar información relevante para el cumplimiento de sus funciones, los organismos de inteligencia pueden realizar actividades conocidas como "operaciones especiales". Respecto de ellas, la legislación peruana da una definición general, entendiendo por ellas "acciones operativas de inteligencia y contrainteligencia, que suponen la trasgresión de determinados derechos ciudadanos, en razón de amenazas a la seguridad nacional, requiriendo previa autorización judicial para su realización" (Ley 28.664, Disposiciones complementarias).

iv. **Procedimiento para la realización de estas actividades:** las operaciones especiales deben ser solicitadas por el director de la Dirección Nacional de Inteligencia; solo excepcionalmente, en casos de peligro para la seguridad nacional y por la urgencia de las circunstancias, puede este autorizarlas directamente, aunque en todo caso debe solicitar la revisión judicial posterior (Ley 28.664, artículo 20)

v. **Controles que pueden ejercerse:** de acuerdo con la Ley 28.664, existen controles internos y externos a las actividades de inteligencia.

En cuanto a los controles internos, se indica que corresponde a una dependencia de la Dirección Nacional de Inteligencia y de cada uno de los órganos que integran el Sistema de Inteligencia Nacional fiscalizar la gestión administrativa, económica y financiera de los recursos y bienes de estas entidades (Ley 28.664, artículo 30).

En cuanto a los controles externos, cabe destacar dos. Por un lado, las llamadas "operaciones especiales" requieren autorización judicial para poder ejercerse, el cual recae en dos vocales superiores ad hoc nombrados por la Corte Suprema de Justicia. Deben ser tramitadas dentro de las 24 horas siguientes a haber sido informadas al juez correspondiente. En circunstancias de peligro para la seguridad nacional y por la urgencia de las circunstancias, tal control podrá ser posterior, caso en el cual debe ejercerse dentro de las 24 horas siguientes a la autorización de la correspondiente operación especial, con el propósito de convalidarla o de ordenar su inmediata paralización. La decisión negativa del vocal que haya conocido de la resolución podrá apelarse ante la Sala de la que haga parte (Ley 28.664, artículo 20).

Por otro lado, el Congreso de la República también tiene la función de fiscalizar las labores de inteligencia, lo cual deberá hacer a través de la Comisión de Inteligencia. Para el cumplimiento de sus funciones, tiene la competencia para solicitar información clasificada o no clasificada a todos los componentes del Sistema de Inteligencia Nacional, así como realizar investigaciones de oficio (Ley 28.664, artículo 21).

c. Vigilancia de las comunicaciones en el marco de investigaciones penales

La legislación peruana admite que las autoridades de investigación penal puedan adoptar determinadas medidas que pueden limitar la confidencialidad de las comunicaciones. Tales medidas se encuentran reguladas principalmente en el Nuevo Código Procesal Penal (en adelante, "NCPP"), promulgado mediante el Decreto Legislativo 957. Lo allí dispuesto en materia de interceptación de comunicaciones se encuentra regulado en la Resolución Nº 4933-2014-MP de la Fiscalía General.

i. **Facultades de las autoridades de investigación que interfieren con las comunicaciones personales:** bajo la categoría de control de comunicaciones y documentos privados, la legislación procesal penal peruana establece tres tipos de medidas: la interceptación e incautación postal; la intervención de comunicaciones y telecomunicaciones; y el aseguramiento e incautación de documentos privados (NCPP, artículos 226 y 234).

   Específicamente con relación a la intervención de comunicaciones y telecomunicaciones, se prevén dos medidas: (i) intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y (ii) registro de la intervención de comunicaciones telefónicas o de otras formas de comunicación (NCPP, artículos 230 y 231).

ii. **Autoridades que pueden ordenar la vigilancia:** corresponde al fiscal de cada caso solicitar la práctica de estas medidas, las cuales deben ser aprobadas por el juez previamente a su realización (NCPP, artículos 230 y 231).

iii. **Circunstancias en las que tales facultades pueden ejercerse:** el fiscal podrá solicitar la intervención de comunicaciones dependiendo de la pena prevista para el delito investigado y de la necesidad de la medida. Así, esta medida procede "cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad y la intervención sea absolutamente necesaria para proseguir las investigaciones" (NCPP, artículo 230).

iv. **Procedimiento que debe seguirse para que se ordene una actuación de vigilancia de comunicaciones:** al realizar la solicitud de intervención de comunicaciones, el fiscal deberá indicar el nombre y dirección del afectado por la medida, al igual que, "de ser posible", la identificación de los medios de comunicación o telecomunicación que se pretende intervenir, grabar o registrar. Asimismo, deberá indicar "la forma de la interceptación, su alcance y su duración, al igual que la autoridad o funcionario, policial o de la propia Fiscalía, que se encargará de la diligencia de interceptación y grabación o registro" (NCPP, artículo 230).

   La intervención de comunicaciones no podrá extenderse por más de 30 días, y excepcionalmente podrá prorrogarse por plazos sucesivos, en cada caso previa solicitud del fiscal y autorización del juez de investigación preparatoria. La medida deberá ser interrumpida una vez se cumpla el plazo para el cual fue autorizada o en caso de que desaparezcan los elementos que tuvo en cuenta el juez para ordenarla (NCPP, artículo 230).

   Los resultados de la interceptación de comunicaciones serán registrados en medios técnicos que aseguren su fidelidad. El registro será entregado al fiscal, quien deberá preservar su confidencialidad (NCPP, artículo 231).

v. **Controles aplicables a la vigilancia de las comunicaciones en materia penal:** es necesaria la autorización judicial previa para que puedan realizarse las medidas de investigación relacionadas con la interceptación de comunicaciones. El encargado de otorgar tal autorización es el juez de investigación preparatoria, quien resolverá la solicitud formulada por el fiscal en un trámite reservado y de forma inmediata, teniendo a la vista los elementos recaudados que justifique el requerimiento del fiscal. En caso de respuesta negativa por parte del juez, la decisión podrá ser apelada (NCPP, artículo 230).

Adicionalmente, se prevé la realización en el más breve plazo de una audiencia judicial en la que podrá examinarse los resultados de la medida y a la que el afectado podrá hacer valer sus derechos (NCPP, artículo 231).

Bibliografía

Bibliografía general

Becker, Sebastián; Lara, Carlos; y Canales, María Paz, "La construcción de estándares legales para la vigilancia en América Latina. Parte I: Algunos ejemplos de regulación actual en América Latina", Derechos Digitales América Latina, septiembre 2018.

Bibliografía por país

Argentina

Ferrari, Verónica y Schnidrig, Daniela. "Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en Argentina", EFF y CELE, Agosto 2016. p. 16.

Brasil

Antonialli, Dennys y de Souza Abreu, Jacqueline. "Vigilancia estatal de las comunicaciones en Brasil y la protección de los derechos fundamentales", EFF & Internet Lab, marzo 2016.

Chile

Lara, J. Carlos y Hernández, Valentina. "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile", EFF & Derechos Digitales, 2016. p. 28. Disponible en: https://www.eff.org/es/country-reports/Chile-ES-final.

Colombia

Rodríguez, Katitza y Rivera, Juan Camilo. "Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia", EFF, 2015. p. 16. Disponible en: https://www.eff.org/files/2015/05/21/vigilancia_de_comunicaciones_colombia_eff.pdf.

México

García, Luis Fernando. "Vigilancia estatal de las comunicaciones y protección de los Derechos Fundamentales en México", EFF & R3D, agosto de 2016.

Panamá

Rodríguez, Katitza y Alimonti, Veridiana. "The State of Communication Privacy Law in Panama", EFF, junio de 2020.

Paraguay

Rodríguez, Katitza y Alimonti, Veridiana. "The State of Communication Privacy Law in Paraguay", EFF, junio de 2020.

Perú

Morachimo, Miguel. "State Communications Surveillance and the Protection of Fundamental Rights in Peru", EFF & Hiperderecho, julio de 2016.

Anexo 1

Régimen constitucional de la vigilancia de las comunicaciones

	Regulación de la inviolabilidad de las comunicaciones
Argentina	Prevé la inviolabilidad de la correspondencia epistolar y de los papeles privados. Señala que puede limitarse por ley que indique los casos y justificativos para proceder al allanamiento y ocupación.
Brasil	Reconoce el derecho a la inviolabilidad del secreto de las comunicaciones, agregando que solo puede limitarse cuando medie orden judicial y en los casos y formas que establezca la ley tratándose de una investigación penal o para instruir procesos penales.
Chile	Reconoce el derecho a la inviolabilidad de las comunicaciones privadas y dispone que para limitarlo debe mediar una ley que especifique los casos y las formas para ese efecto.
Colombia	Indica que la correspondencia y demás formas de comunicación privada son inviolables, especificando que estas pueden ser interceptadas o registradas mediante orden judicial y en los casos y con las formalidades que establezca la ley.
México	Establece el derecho a la inviolabilidad de las comunicaciones y regula un amplio catálogo de garantías relacionadas con este derecho. Entre las más destacables se encuentran las siguientes: el deber de sancionar el desconocimiento de la libertad o secreto de las comunicaciones; la reserva judicial para la intercepción de cualquier comunicación privada, indicando que debe ser autorizada por una autoridad judicial federal, a petición de la autoridad federal que señale la ley o del titular del Ministerio Público de una entidad federativa, fundada en causas legales; el deber de la autoridad federal correspondiente de motivar la solicitud y de identificar con precisión la persona afectada, la duración y los medios; y algunos tipos de asuntos sobre los cuales no podrá proceder la intervención de comunicaciones (a saber: cuestiones de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni las comunicaciones del detenido con su defensor).
Panamá	Establece que la correspondencia y los demás documentos privados son inviolables, por lo que no pueden ser examinados ni retenidos, sino mediando orden de autoridad competente y para fines concretos, en cumplimiento de las formas que prevea la ley. Agrega que debe guardarse absoluta reserva con relación a los asuntos ajenos al objeto del examen o retención.
Paraguay	Reconoce la inviolabilidad de las comunicaciones telefónicas, telegráficas, cablegráficas o de cualquier otra especie. Añade que, como consecuencia, tales comunicaciones no pueden ser examinadas, reproducidas, interceptadas o secuestradas, excepto en el caso de que exista orden judicial, de que se trate de cuestiones específicas previstas en la ley y que se trate de información indispensable para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades.
Perú	Reconoce la inviolabilidad de las comunicaciones, telecomunicaciones y sus instrumentos. Dispone que ellos solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado de un juez, siguiendo las garantías previstas en la ley. La anterior excepción a la inviolabilidad de las comunicaciones debe limitarse a aquellos asuntos que motivaron su examen. También se excluye valor probatorio a los documentos que no hubieran sido obtenidos en cumplimiento de lo previsto en este artículo.

Anexo 2

Relevancia de los tratados internacionales de derechos humanos en el ordenamiento jurídico interno

	Relevancia jurídica en el ordenamiento interno a los tratados internacionales de derechos humanos
Argentina	Reconoce jerarquía constitucional a un amplio catálogo de tratados de derechos humanos, que se encuentran expresamente previstos en la Constitución.
Brasil	Reconoce jerarquía constitucional a los tratados de derechos humanos aprobados por el Congreso Nacional por una mayoría especial de sus miembros.
Chile	Reconoce jerarquía constitucional a los tratados de derechos humanos ratificados por Chile y que se encuentren vigentes.
Colombia	Reconoce jerarquía constitucional a los tratados de derechos humanos "***atificados por el Congreso, que reconocen los derechos humanos y que prohíben su limitación en los estados de excepción***", mientras que indica que todos los tratados internacionales sobre derechos humanos ratificados por Colombia deberán tenerse en cuenta para la interpretación de los derechos previstos en la Constitución.
México	Reconoce jerarquía constitucional a los tratados de derechos humanos en los que el Estado mexicano sea parte.
Panamá	No existe una cláusula específica que haga referencia al valor normativo de los tratados internacionales sobre derechos humanos.
Paraguay	Reconoce a los tratados, convenios y acuerdos internacionales aprobados y ratificados un valor infra-constitucional, pero superior al de las leyes.
Perú	Asigna a los tratados internacionales en general el rango de ley.

Anexo 3

Aspectos destacados en la regulación sobre vigilancia de las comunicaciones en labores de inteligencia

	Límites expresos a las actividades de inteligencia	Facultades que pueden realizar los organismos de inteligencia con el propósito de obtener información	¿Procede control judicial para autorizar la realización de actividades de inteligencia?
Argentina	Ningún organismo de inteligencia podrá cumplir funciones policiales o de investigación criminal, tener en cuenta en la realización de sus funciones motivaciones discriminatorias, buscar influenciar en la vida política, institucional, militar, social o económica del país, ni revelar o divulgar información adquirida en el ejercicio de sus funciones (salvo que medie orden judicial).	▪ Interceptación o captación de comunicaciones privadas de cualquier tipo.	Sí, para el caso de la interceptación y captación de comunicaciones privadas de cualquier tipo. En este caso, el control es previo.
Brasil	Las actividades de inteligencia deben llevarse a cabo con "respeto irrestrictico por los derechos y garantías individuales, con lealtad a las instituciones que rigen los intereses y la seguridad del Estado".	La única facultad que la legislación especifica relacionada con la recolección o producción de información relevante para la realización de funciones de inteligencia es la de acceder, por medios electrónicos, a bases de datos de los órganos a los que pertenecen.	No se prevé control judicial para el desarrollo de esta actividad.
Chile	Se establece que las actividades de inteligencia deben desarrollarse con apego a la Constitución Política y a las leyes	Tratándose de la obtención de información no disponible en fuentes abiertas, se prevén etas facultades: ▪ Intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas. ▪ Intervención de sistemas y redes informáticos ▪ Escucha y grabación electrónica incluyendo la audiovisual ▪ Intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.	Control judicial previo con relación a todos los procedimientos antes mencionados relacionados con la obtención de información que no se encuentre disponible en fuentes abiertas.

Colombia	Las labores de inteligencia solo pueden ser realizadas con el propósito de proteger determinadas finalidades, señaladas en la ley de inteligencia colombiana; no pueden ser utilizadas con propósitos discriminatorios; y al decidirse sobre su realización debe analizarse que se cumplan los principios de necesidad, idoneidad y proporcionalidad.	Se regula expresamente dos facultades que pueden ejercer los organismos de inteligencia para el cumplimiento de sus funciones: ▪ Monitoreo del espectro electromagnético, la cual es distinta de la interceptación de comunicaciones personales. Esta última no puede ser realizada para fines de inteligencia. ▪ Requerir a los operadores de servicios de telecomunicaciones información que ayude a la identificación y localización de los usuarios de estos servicios.	Las dos actividades mencionadas no requieren control judicial previo para su realización.
México	Se indica de forma general que, al utilizar cualquier método de recolección de información, las autoridades de inteligencia deben respetar las garantías individuales y los derechos humanos	Las instancias de inteligencia podrán hacer uso de cualquier método de recolección de información. Además, la legislación mexicana hace referencia a una facultad específica que permite la recolección de información de inteligencia y que limita la confidencialidad de la información. Se trata de la intervención de comunicaciones privadas, aplicable a "comunicaciones y emisiones privadas, realizadas por cualquier medio de transmisión, conocido o por conocerse, o entre presentes, incluyendo la grabación de imágenes privadas".	La intervención de comunicaciones por razones de inteligencia requiere de autorización judicial.
Panamá	Se establecen prohibiciones generales para la Secretaría Ejecutiva del Consejo de Seguridad Nacional, que es el órgano que, entre otras funciones, desempeña labores de inteligencia. Tales prohibiciones son las siguientes: vulnerar los derechos consagrados en la Constitución y en las leyes; la participación en cualquier actividad política partidista; difundir cualquier información que hubiera conocido debido a sus actividades; cualquier otra actividad que atente contra la integridad física y moral, honra y bienes de los asociados; y la realización de actividades que involucren espionaje político.	Solicitar a las personas naturales o jurídicas los datos, estadísticas e informaciones que estén relacionadas con la seguridad nacional, así como a prestar apoyo y colaboración necesaria	No se especifica el control que los jueces podrán realizar con relación a las funciones de inteligencia que puedan afectar la confidencialidad de las comunicaciones.

Paraguay	Las labores de inteligencia no pueden ejercerse con propósitos discriminatorios, ni para influir en la situación institucional, política, militar, policial, social o económica del país, ni para realizar labores represivas, de policía o de investigación criminal, ni para revelar o divulgar información obtenida en el marco de sus actividades.	Se establecen los siguientes procedimientos específicos de obtención de información: ▪ Intervención de comunicaciones telefónicas, informáticas, radiales y de correspondencia en cualquiera de sus formas. ▪ Intervención de sistemas y redes informáticas. ▪ Escucha y grabación electrónica audiovisual. ▪ Intervención de cualquier otro sistema tecnológico destinado a la transmisión, almacenamiento o procesamiento de comunicaciones o información.	La autorización de los llamados procedimientos específicos de obtención de información debe realizarla un juez de control de garantías.
Perú	Se establece una serie de principios operativos para el funcionamiento de los servicios de inteligencia: legalidad, legitimidad, control democrático, pertinencia, circulación restringida, especialidad y planificación.	Los organismos de inteligencia pueden realizar, entre otras, "operaciones especiales", entendidas como acciones operativas de inteligencia y contrainteligencia, que suponen la trasgresión de determinados derechos ciudadanos, debido a amenazas a la seguridad nacional, requiriendo previa autorización judicial para su realización	Las llamadas "operaciones especiales" requieren autorización judicial para poder ejercerse.

Anexo 4

Aspectos destacados en la regulación sobre vigilancia de las comunicaciones en el marco de procesos penales

	Medidas de investigación penal que interfieren con la inviolabilidad de las comunicaciones	¿Cómo opera el control judicial con relación a estas medidas?
Argentina	Interceptación y secuestro de correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a éste, aunque sea bajo nombre supuesto	Control judicial previo.
Brasil	▪ Interceptación de las comunicaciones que transcurren vía tecnologías de información y medios telemáticos. ▪ Captura ambiental de señales electromagnéticas, ópticas o acústicas. ▪ Deber de las concesionarias de telefonía móvil y fija de mantener por cinco años a disposición del jefe de la Policía Civil y la Fiscalía General "los registros para identificar los números de terminales entrantes y salientes de llamadas internacionales, de larga distancia o locales". ▪ El jefe de la Policía Civil y la Fiscalía General podrán acceder a cierta información sobre la cuenta que tengan, entre otras entidades, las compañías telefónicas y las proveedoras de internet.	La interceptación de comunicaciones telefónicas requiere de autorización judicial previa. Igualmente, una vez realizada la diligencia de interceptación, el juez debe decidir si los resultados son relevantes para la investigación, existiendo así también un control judicial posterior. También con relación a la captura ambiental de señales electromagnéticas, ópticas o acústicas procede el control judicial previo y posterior.
Chile	▪ Retención e incautación de correspondencia postal, telegráfica o de otra clase y de los envíos dirigidos al imputado o remitidos por él, o de aquéllos de los cuales se presumiere que emanan de él o de los que él pudiere ser el destinatario. ▪ Interceptación y grabación de las comunicaciones telefónicas o de otras formas de telecomunicación.	Dado que se dispone que toda actuación que prive al procesado de sus derechos, o los restrinja o perturbe, requiere autorización judicial previa por parte del juez de control de garantías, estas dos medidas requieren de este tipo de control.
Colombia	▪ Interceptación, mediante grabación magnetofónica o similares, de las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. ▪ Aprehensión de los equipos y medios de almacenamiento que pudieran haber sido utilizados por el investigado para transmitir información útil para la investigación que se adelante a través de internet u otros medios tecnológicos que produzcan efectos equivalentes. ▪ Retención de correspondencia privada, postal, telegráfica o de mensajería especializada o similar.	El control judicial a las medidas antes mencionadas es posterior, dentro de las 24 horas siguientes al diligenciamiento de las órdenes correspondientes.

México	▪ Intervención de comunicaciones privadas, abarca todo sistema de comunicación o programa 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". ▪ Geolocalización y solicitud de entrega de datos conservados.	En relación con la intervención de comunicaciones privadas, el juez decidirá si la autoriza. Asimismo, podrá en cualquier momento verificar que sea realizada en los términos autorizados y, en caso de incumplimiento, decretar su revocatoria parcial o total. Por otro lado, una vez concluida la diligencia, la Fiscalía General de la Nación informará al juez. En cuanto a la entrega de información para geolocalización y la entrega de datos conservados, existe control judicial previo por parte del juez de control competente. No obstante, en determinadas circunstancias, la medida puede ser ordenada directamente por el Fiscal General de la República o quien sea delegado para este efecto, caso en el cual el control judicial será posterior.
Panamá	▪ Incautación de correspondencia. ▪ Grabación de conversaciones e interceptación de comunicaciones cibernéticas, seguimientos satelitales, vigilancia electrónica y comunicaciones telefónicas.	El juez de control de garantías debe conceder la realización de estas medidas de investigación.
Paraguay	▪ Intercepción y secuestro de correspondencia. ▪ Intervención de las comunicaciones del acusado, cualquiera fuera el medio técnico empleado.	Existe control judicial previo de las medidas restrictivas de la inviolabilidad de las comunicaciones.
Perú	▪ Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación. ▪ Registro de la intervención de comunicaciones telefónicas o de otras formas de comunicación.	Es necesaria la autorización judicial previa para que puedan realizarse las medidas de investigación relacionadas con la interceptación de comunicaciones.

www.alsur.lat

AlSur