Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica

Katitza Rodríguez Pereda

Octubre 2016

ELECTRONIC FRONTIER FOUNDATION

La autora principal del *Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica* es la Directora International de Derechos Humanos de la Electronic Frontier Foundation (EFF), Katitza Rodríguez Pereda. La revisión legal fue realizada por el Director de Libertades Civiles, David Greene. La revisión técnica fue realizada por el tecnólogo senior de EFF, Seth Schoen. La Administradora de Proyectos Internacionales de la EFF, Kim Carlson, editó y realizó la corrección de estilo. EFF quiere agradecer a Juan Camilo Rivera, consultor del EFF para este proyecto, y Ana María Acosta, 2016 Google Policy Fellow por sus contribuciones en la elaboración del presente informe.

EFF desea agradecer a las siguientes personas por su valiosa contribución, asistencia, y retroalimentación en la preparación de la investigación:

Agustina Del Campo, Centro de Estudios en Libertad de Expresión y Acceso a la Información (Argentina)
Ana Tuduri (Uruguay)
Carolina Botero, Fundación Karisma (Colombia)
Daniela Schnidrig, Global Partners Digital (Argentina)
Dennys Antonialli, InternetLab (Brazil)
Fabrizio Scrollini (Uruguay)
Jacqueline Abreu, Internet Lab (Brazil)
Jorge Gabriel Jímenez (Guatemala)
Juan Carlos Lara, Derechos Digitales (Chile, Latin America)
Juan Diego Castañeda Gómez, Fundación Karisma (Colombia)
Leandro Ucciferri, Asociación por los Derechos Civiles (Argentina)
Luciana Peri, Fundación Acceso (Centro América)
Luis Fernando García, Red en Defensa de los Derechos Digitales (México)
Maricarmen Sequera, TEDIC (Paraguay)
Marlon Hernández Anzora (El Salvador)
Miguel Morachimo, Hiperderecho (Peru)
Verónica Ferrari, Centro de Estudios en Libertad de Expresión y Acceso a la Información (Argentina)

También nos gustaría dar las gracias al personal y consultores de la EFF que contribuyeron substantivamente al éxito de este proyecto:

Carlos Wertheman, Editor en Español de la EFF
Danny O'Brien, International Director
David Bogado, ex coordinador de la EFF en Latinoamérica (Paraguay)
Justina Díaz Cornejo, traductora
Sara Fratti, traductora
Ramiro Ugarte, asesor legal

Los siguientes informes son parte de un proyecto regional llevado a cabo por la EFF en 12 países de América Latina y han sido utilizados como fuentes principales para el "Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica."

Ana Tudurí, Fabrizio Scrollini, y Katitza Rodríguez, "*Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay*," Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/uruguay

Daniela Schnidrig y Verónica Ferrari, "*Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina,*" Electronic Frontier Foundation y Centro de Estudios en Libertad de Expresión y Acceso a la Información, (2016). https://necessaryandproportionate.org/country-reports/argentina

Dennys Antonialli y Jacqueline de Souza Abreu, "*Vigilancia estatal de las comunicaciones en Brasil y la protección de los derechos fundamentales,*" Electronic Frontier Foundation y InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

Fundación Acceso, "*¿Privacidad digital para defensoras y defensores de derechos humanos?, un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos,*" Peri, Luciana (coord.). -- 1a. ed.-- San José, C.R.: Fundación Acceso, 2015. https://necessaryandproportionate.org/files/2016/05/16/investigacion-privacidad-digital-fa.pdf

Jorge Rolón Luna y Maricarmen Sequera, "*Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay,*" Electronic Frontier Foundation y TEDIC, (2016). https://necessaryandproportionate.org/country-reports/paraguay

Juan Camilo Rivera y Katitza Rodriguez, "*Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en Colombia,*" Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

Juan Carlos Lara y Valentina Hernández, "*Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile,*" Electronic Frontier Foundation y Derechos Digitales, (2016). https://necessaryandproportionate.org/country-reports/chile

Luis Fernando Garcia, "*Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México,*" Electronic Frontier Foundation y InternetLab, (2016). https://necessaryandproportionate.org/country-reports/mexico

Miguel Morachimo, "*Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú*," Electronic Frontier Foundation & Hiperderecho, (2016). https://necessaryandproportionate.org/country-reports/peru

Índice de contenido

Introducción

En diciembre de 1992, y siguiendo el boceto de un mapa que le entregó un "whistleblower", el abogado paraguayo Martín Almada condujo a una oscura estación de policía en el suburbio de Lambaré, cerca de Asunción. Detrás de las oficinas de la policía, en un edificio de oficinas en decadencia, Almada descubrió, apilados casi hasta el techo, un alijo de 700.000 documentos. Estaba frente al "Archivo del Terror", un registro casi completo de interrogatorios, torturas, y vigilancia llevada a cabo por la dictadura militar de Alfredo Stroessner. Estos archivos revelaron detalles de la "Operación Cóndor", un programa clandestino entre las dictaduras militares en Argentina, Chile, Paraguay, Bolivia, Uruguay y Brasil durante la década comprendida entre 1970 y 1980s.[1] Los gobiernos militares de estos países acordaron cooperar en el envío de equipos a otros países para rastrear, monitorear y asesinar a sus oponentes políticos.[2] Los archivos listan más de 50,000 muertes y 400,000 prisioneros políticos en toda Argentina, Bolivia, Brasil, Chile, Paraguay, Uruguay, Colombia, Perú y Venezuela.[3]

La policía secreta de Stroessner usaba informantes, cámaras con teleobjetivo y escuchas telefónicas para construir una base de datos de todos los que fueran visto como una amenaza, además de sus amigos y asociados. Almada mismo, había sido torturado por el régimen y su esposa murió de un ataque al corazón luego de que la policía le pusiera, en el teléfono, los gritos de su esposo en la cárcel. El Archivo del Terror es una muestra de cuán bajo puede caer el gobierno de un país cuando no está controlado por autoridades judiciales imparciales e independientes, órganos de supervisión pública autónomos y por el público en general.

Un Stroessner de nuestros días o una nueva Operación Cóndor, claramente, tendrían herramientas muchas más poderosas a la mano que meros cuadernos anillados, cámaras y teléfonos interceptados. La vigilancia digital de las telecomunicaciones en la actualidad hacer ver a las documentadas en el Archivo del Terror como reliquias. Las nueva tecnologías, como los IMSI-catchers, una torre celular portátil que posibilita a su operador barrer todas las comunicaciones de teléfonos y mensajes dentro de un radio de 200 metros, permiten a las autoridades recolectar la identidad de todos los asistentes a las protesta. Los teléfonos móviles constantemente informan a las empresas proveedoras dónde se encuentran todo el tiempo, el gobierno puede exigir a estas empresas retener los datos y solicitar el acceso a los mismos. Eso permitiría a las autoridades realizar un seguimiento de los movimientos de cada usuario de celular. También les permitiría un "viaje en el tiempo", escoger un objetivo y

1 Paraguay's Archive Terror, http://news.bbc.co.uk/2/hi/americas/1866517.stm

2 Condor legacy haunts South America, http://news.bbc.co.uk/2/hi/3720724.stm

3 1992: Archives of Terror Discovered, http://nationalgeographic.org/thisday/dec22/archives-terror-discovered/

después buscar en su historial las ubicaciones donde han estado en los últimos años.

Para una intimidación particularizada, los gobiernos podrían tomar ventajas de los emails, redes sociales y mensajes que dominan nuestras vidas. Los Estados podrían implementar, como mecanismo de control social, el mismo software malicioso, o malware, que los delincuentes de poca monta utilizan para tomar control sobre los equipos de usuarios inocentes, engañándoles para que accedan a correos y websites fraudulentos. Alguno de aquellos programas maliciosos son también "spyware" - capaces de grabar, encubiertamente, audio y video de micrófonos, cámaras del teléfono inteligente y laptop del objetivo. Una vez instalado, el malware del gobierno podría ir mucho más lejos, como recuperar la lista de contactos o remotamente implantar evidencia incriminatoria en el dispositivo. Una red mucho más amplia y más perversa que cualquier proyecto de la policía secreta del siglo XX que sería utilizado sobre toda la sociedad.

La perturbadora verdad es que dichas herramientas no son teóricas. Muchos gobiernos ya las están usando, sin las limitaciones legislativas que los controlen y sin ningún tipo de supervisión pública eficaz, como lo demuestra nuestra investigación.

Fue necesaria una filtración en uno de los proveedores de malware más notorios del mundo, el italiano "Hacking Team" y el cuidadoso trabajo de periodistas de investigación, para revelar cómo muchos gobiernos latinoamericanos ya estaban usando la vigilancia masiva y otras herramientas invasivas como el malware comercial. Los IMSI catchers a veces se insinúan en documentos judiciales. En ocasiones raras y aleatorias se requiere a los tribunales aprobar el uso de tal mecanismo de vigilancia, sin embargo, los jueces a menudo no conocen el poder y el alcance de estas nuevas herramientas tecnológicas.

Las leyes de vigilancia del siglo XX simplemente regulan la interceptación de las comunicaciones de una línea telefónica particular, sin ninguna guía sobre cómo aplicar estas leyes frente al incremento en el uso de las nuevas técnicas y tecnologías de espionaje. Cuando nuevas leyes de vigilancia o de seguridad cibernética se aprueban, su propósito básico es legitimar las prácticas existentes, o ampliar los poderes existentes, tales como las leyes de retención de datos que obligan a las empresas de telefonía y proveedores de acceso a Internet a registrar y, aún más, conservar datos de una población entera para uso estatal.

Cada uno de estos nuevos poderes es una bomba de tiempo por detonar. La única manera de evitar su uso en contra de la gente es crear leyes modernas, sólidas y detalladas que limiten su uso, además, es necesario contar con un poder judicial independiente, que evalúe y haga cumplir esos límites, y mecanismos de supervisión pública que posibiliten a la población saber lo que los servicios secretos de su país realizan en su nombre, y asegurarse que las garantías se cumplan.

Desafortunadamente, los legisladores y jueces dentro de América Latina y más allá tienen

poca idea de cómo la leyes de vigilancia existente son deficientes, o cómo podrían ser reformadas.

Para ayudar en esa tarea imponente, la Electronic Frontier Foundation ha pasado más de un año trabajando con nuestras organizaciones aliadas en toda América Latina. Nuestra intención era dar luz a las actuales actividades de vigilancia, en la legislación y en la práctica. Hemos documentado cuidadosamente la legislación vigente en 12 países de América Latina y Estados Unidos, y hemos reunimos evidencia de su mala aplicación siempre que sea posible.

Nuestro objetivo, con estos documentos, es comparar las prácticas y leyes existentes con los estándares establecidos de derechos humanos. Sin esas limitaciones legales, todos los países, dentro de América Latina y por fuera, no sólo corren el riesgo de violar los derechos de sus propios ciudadanos, sino que ponen en peligro el ser derrocados por elementos ilegítimos en su propia sociedad, impulsados por una policía secreta técnicamente equipada.

En nuestra investigación, evaluamos las leyes y regulaciones de acceso público. Dada la arraigada cultura del secreto que rodea la vigilancia, es muy difícil juzgar el grado en que los Estados cumplen con sus propias normas legales publicadas. Asegurar, no solo, que la ley cumple con las normas de derechos humanos, sino que también gobierna efectivamente y describe el comportamiento de los estados en el mundo real es un desafío permanente.

Los funcionarios del Estado y la sociedad civil deben asegurarse que las normas escritas sean aplicadas consistentemente en la práctica y que las fallas al hacer cumplir la ley sean descubiertas y remediadas. Esto plantea un segundo problema: la falta de supervisión pública adecuada en toda la región. Esta es la razón principal por la que incluso garantías positivas establecidas por la ley - y existen muchos ejemplos de buenas normas de vigilancia en la región - simplemente no funcionan. Estas sólo pueden ser superadas si la sociedad civil exige transparencia y rendición de cuentas de los servicios de inteligencia y la policía.

Los esfuerzos de supervisión pública suelen ser superados por el secreto que rodea las actividades de inteligencia y la policía. Sin embargo, los avances producidos en la última década en leyes de acceso a la información en toda la región ofrecen la oportunidad de penetrar a través de estos obstáculos y reforzar el control de los ciudadanos sobre una parte del Estado, que permanece en la oscuridad.

Nuestro mensaje no es completamente pesimista. Nuestro análisis ha descubierto procedimientos legales que buscan preservar los derechos humanos, al menos en teoría, y que están un paso por delante del resto del mundo. Ahora tenemos que asegurarnos que esas leyes efectivamente se cumplan. En el resumen a continuación, enumeramos tanto lo bueno y lo malo de las leyes de vigilancia moderna latinoamericana. Cada Estado puede mejorar, pero muchos podrían beneficiarse al imitar de las experiencias positivas de otras jurisdicciones.

La tecnología no puede defendernos, completamente, del mal uso de estas nuevas herramientas y capacidades. Necesitamos un fuerte Estado de Derecho, reglamentos robustos que sean, realmente, prescritos por ley, necesarios, adecuados y proporcionados. Necesitamos autorización judicial, debido proceso, transparencia y el derecho a ser notificado de la decisión de vigilancia con tiempo e información suficientes para impugnar la decisión o buscar otras soluciones siempre que sea posible. Necesitamos vías de reparación para los afectados por las medida de vigilancia.

Además de tener un diseño institucional para una mejor supervisión y control de estas actividades, la región debe comprometerse a mejorar la independencia de su Poder Judicial e implementar mecanismos de supervisión pública que cuenten con recursos, conocimientos del tema, y autoridad legal suficiente sobre aquellos que ejerzan los poderes de vigilancia. También necesitamos una fuerte coalición en la sociedad civil que observe a quienes nos observan, que vigile a quienes nos vigilan. Con la ayuda de jueces y legisladores vigilantes e informados, esperamos que la tecnología digital se utilice sabiamente para proteger, y no violar, los derechos humanos. Debemos asegurarnos que podemos construir un mundo en el que el Archivo del Terror siga siendo un triste registro de errores pasados, no un presagio de baja tecnología de un futuro aún más oscuro.

Resumen Ejecutivo

La Constitución de cada país latinoamericano reconoce el derecho a la privacidad de cierta forma: comúnmente como un derecho general a la vida privada o intimidad. A veces es protegido como múltiple, derechos específicos: el derecho a la inviolabilidad de las comunicaciones; como el derecho a la protección de datos o el derecho de hábeas data, que varía de un país a otro, pero en general, el hábeas data protege el derecho de toda persona a conocer la información que se guarda sobre su persona.

Desafortunadamente, a pesar de este consenso, la mayoría de los estados no han incorporado estos derechos de una manera que cumplan plenamente con los estándares internacionales de derechos humanos.

Los "Principios Necesario y Proporcional" proveen la base principal para evaluar si las prácticas de vigilancia e interceptación de comunicaciones de un estado se ajustan a los estándares internacionales de derechos humanos. En este trabajo, evaluamos hasta qué punto las leyes y prácticas de vigilancia estatal de las comunicaciones en 13 países de Latinoamérica se ajustan (o no) a los Principios. Usando este análisis, identificamos las mejores prácticas que deberían servir como modelo para los estados, así como las reformas específicas y necesarias para llevar a la ley y la práctica al cumplimiento de los estándares de derechos humanos.

Nuestro reporte también identifica las deficiencias que se han extendido a lo largo de la región y que merecen especial e inmediata atención. América Latina aparece con un retraso en comparación al resto del mundo al permitir regulaciones que exijan la retención obligatoria de datos personales por parte de las empresas proveedoras de Internet y telefónicas. Eso contrasta, por ejemplo, con Europa, cuya propia Directiva Europea de Retención de Datos ha sido anulada luego de un exitoso desafío legal basado en derechos humanos. Tampoco el derecho en los países latinoamericanos ha podido mantenerse al día respecto al siempre creciente alcance de lo que constituye la "vigilancia de las comunicaciones". Como resultado, las nuevas tecnologías de vigilancia, como los IMSI catchers[4] y malware,[5] son de uso generalizado mas no existe autorización legal específica ni

4 Simuladores de torre celulares, conocidos comúnmente como IMSI-catchers o Stingrays, son dispositivos que se hacen pasar por una torre de telefonía celular legítima, engañando los teléfonos móviles cercanos para que se conecten al dispositivo con el fin de registrar la identidad del abonado móvil de los teléfonos en la zona o capturar el contenido de las comunicaciones. Más información en: https://www.eff.org/sls/tech/cell-site-simulators

5 El software maliciosos funciona de muchas formas diferentes: altera el funcionamiento del equipo, recopila información sensible, se hace pasar por un usuario para enviar mensajes de spam o falsos, y accede a los sistemas informáticos privados. Más información en:

garantías adecuadas para la protección de derechos humanos. Los estados, también, no han logrado ampliar el alcance de las leyes de vigilancia para eliminar las distinciones anticuadas entre el contenido de las comunicaciones y otros metadatos de comunicaciones.

El Principio de Legalidad

El principio de legalidad requiere que cualquier limitación a los derechos humanos sea prescrita por la ley, y que la ley sea pública, precisa y sin ambigüedades. El estado, por tanto, no debe interferir con el derecho a las comunicaciones privadas en ausencia de la existencia de una ley pública que sea suficientemente clara para garantizar que los individuos puedan prever su aplicación. La historia muestra que las leyes imprecisas en materia de inteligencia son propensas al abuso.

Nuestra revisión de las prácticas y leyes de los gobiernos latinoamericanos encontró que muchos estados únicamente autorizan las interceptaciones telefónicas -y no tienen autorización legal precisa para llevar a cabo nuevas formas de vigilancia, como el seguimiento de geolocalización (location tracking), monitoreo de antenas de telefonía móvil (cell tower monitoring), o el uso de IMSI catchers (torres de celular falsas que interceptan las señales telefónicas móviles) o software malicioso (malware). Al igual que las escuchas telefónicas, estas tecnologías son invasivas y subrepticias, pero también plantean muy diferentes preocupaciones y dudas legales que las tradicionales escuchas telefónicas. A pesar de la falta de base legal, estas nuevas tecnologías parecen ser de uso generalizado por las autoridades. El malware, por ejemplo, se conoce que ha sido utilizado en México, Panamá, Venezuela, Colombia, Brasil, Chile, Ecuador, Honduras y Paraguay con autorización legal insuficiente.

También encontramos que muchas prácticas de interceptación y vigilancia de las comunicaciones fueron autorizadas únicamente por el poder ejecutivo en forma de decretos y resoluciones administrativas. Esto incluye mandato de retención de datos en Brasil, Colombia, Perú y Honduras: regulaciones que están vinculadas con disposiciones que permiten a los investigadores públicos amplío acceso a estos almacenes de información privada. Las órdenes ejecutivas que autorizan la vigilancia o prescriben retención de datos son típicamente emitidas sin ningún debate público o inclusión del legislativo o judicial. Algunas directrices acerca de la colaboración entre el sector privado y el gobierno se mantienen en secreto, incluyendo los reglamentos y decretos confidenciales en El Salvador, Uruguay y Perú. A pesar que la retención de datos es en sí misma una medida innecesaria y desproporcionada, México, al menos, proporciona un esbozo de “buena práctica” aquí, con un mandato de retención de datos que es controversial mas fue adoptado por un decreto legislativo público, y cuenta con una precisa lista de datos que deben conservarse.

---

https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware

Incluso cuando la vigilancia se codifique en actos legislativos y otras leyes públicas, esas normativas con frecuencia sufren de vaguedad y ambigüedad. Estas leyes no son suficientemente claras acerca de las facultades específicas que las agencias de inteligencia y la aplicación de la ley poseen para vigilar las comunicaciones. Las leyes a menudo no logran identificar las situaciones apropiadas cuando la vigilancia puede llevarse a cabo o qué entidad específica está facultada para llevar a cabo una forma específica de vigilancia o acceder a comunicaciones recabadas.

Fuera de México, los mandatos de retención de datos no especifican claramente qué datos deben conservarse. Las leyes peruanas que autorizan el seguimiento de localización normalmente no describen qué delitos pueden ser investigados mediante dicha técnica. Las leyes hondureñas no describen que agencias tienen acceso a los datos conservados, mientras que en Colombia el decreto que autoriza la retención de datos permite el acceso a "otras autoridades competentes"; Sin embargo, como resultado de una denuncia ciudadana, la frase "otras autoridades competentes" fue derogada. La decisión de un Consejo de Estado en 2016 cerró esta laguna legal.[6] Ahora sólo el fiscal general (Fiscalía de la Nación), a través de las agencias de la policía judicial, pueden acceder a los datos conservados.

En Colombia, La ley 1621, que regula las actividades de inteligencia, también define vagamente la vigilancia de las comunicaciones, dejando un amplio margen para un potencial abuso. Posteriormente, la Corte Constitucional de Colombia interpretó estas imprecisiones como una autorización para permitir que las agencias de inteligencia puedan monitorear todo el espectro electromagnético con independencia de los medios tecnológicos empleados.[7] Pero esta ley no autoriza explícitamente la vigilancia masiva: En virtud de la jurisprudencia bajo la cual se aprobó la nueva ley de inteligencia de Colombia, el Tribunal Constitucional hace hincapié en que la interceptación sólo es permisible durante una investigación criminal y con autorización judicial. Bajo esta ley, las agencias de inteligencia sólo se les permite monitorear el espectro, que es teoricamente diferente a interceptar las comunicaciones, de acuerdo al Tribunal. La ley no define “el monitoreo del espectro” pero en tanto la Ley 1621 establece claramente que “el monitoreo no constituye intercepción”, una frase que puede ser interpretada ampliamente, es bastante probable que la ley puede ser usada con ese mismo propósito. De hecho, esto puede haber ocurrido ya: en los últimos años, y sin ninguna autorización legal aparente, se han articulado varios programas de vigilancia de masiva. Estos programas se extenderán, supuestamente, a través de mecanismos tales como la Plataforma Única de Monitoreo y Análisis (PUMA) y el Sistema Integral de Grabación Digital, SIGD].

6 “Tumban polémico decreto sobre acceso a datos privados,” Semana Económica, 2016. http://www.semana.com/nacion/articulo/consejo-de-estado-solo-la-fiscalia-podra-tener-acceso-a-datos-privados/465546

7 Comisión Europea, Comité Científico, Terminología técnica – Glosario. http://ec.europa.eu/health/opinions/es/lamparas-bajo-consumo/glosario/def/espectro-electromagnetico.htm

También existe falta de claridad en las garantías de privacidad que algunas leyes proveen. Estas protecciones están plagadas de ambigüedades que pueden ser interpretadas como que autorizan una amplia gama de tecnologías de vigilancia existentes, incluyendo malware e IMSI catchers, y cualquier tecnología de vigilancia futura. Por ejemplo, en Paraguay, el artículo 200 del Código de Procedimiento Penal establece que un juez puede ordenar la interceptación de las comunicaciones de los acusados, "independientemente de los medios técnicos empleados" para lograrlo. En Guatemala, la ley sobre control y prevención de lavado de dinero autoriza el uso de cualquier medio tecnológico disponible para la investigación de los delitos que faciliten su aclaración. El marco de inteligencia argentino permite excepciones significativas a la protección constitucional de privacidad en los "estados de emergencia", una frase que no está definida adecuadamente.

El Principio de Objetivo Legítimo

Este principio requiere que las infracciones en materia de derechos humanos sirvan un propósito legítimo específico que corresponde a un interés jurídico que es necesario en una sociedad democrática. La discriminación es categóricamente un objetivo ilegítimo. Por lo tanto, el principio requiere que cualquier medida que interfiera con un derecho humano no sea promulgada con el propósito o se aplique de una manera que discrimine por motivos de raza, color, sexo, lenguaje, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición. El objetivo legítimo debe operar para limitar la restricción de derechos impuesta por el estado, no debe utilizarse como una excusa para conceder al estado mayor libertad de acción.

En lo que respecta a las infracciones del derecho a la privacidad de las comunicaciones, la investigación de delitos graves, amenazas concretas a la seguridad nacional son reconocidas como objetivos legítimos. La vigilancia de las comunicaciones no puede ser justificada por referencia a un interés general, como la "seguridad", o a una preocupación por la "seguridad nacional", abstracta e indefinida. Las mejores prácticas en esta área comprenden la legislación de vigilancia que contiene una lista exhaustiva de delitos enumerados (o alguna otra definición clara y objetiva) y otras limitaciones legales para asegurar que no ocurran violaciones a los derechos humanos.

El reporte identifica varios ejemplos favorables. Nicaragua, Guatemala y Perú limitan la interceptación de las comunicaciones a la investigación de delitos graves específicos que son enumerados en las normas. Otros estados, sin embargo, como Argentina y Chile, no definen adecuadamente términos tales como "terrorismo", ni especifican que tan grave debe ser la sospecha de un delito para autorizar la vigilancia de las comunicaciones. Como resultado, las consideraciones políticas, subjetivas, arbitrarias y/o inadecuadas pueden dictar cuando estas medidas son utilizadas.

Colombia define adecuadamente la investigación de los delitos de los cuales puede ayudarse por la vigilancia de las comunicaciones, pero no proporciona la misma especificidad y claridad al respecto de las operaciones de inteligencia.

Los Principios de Necesidad, Idoneidad y Proporcionalidad

El principio de necesidad requiere que todas las leyes, reglamentos y actividades que interfieran con los derechos humanos sean limitadas a lo que es estricta y demostrablemente necesario para alcanzar un objetivo legítimo. La vigilancia se debe llevar a cabo cuando es el único medio disponible para alcanzar un objetivo legítimo o, cuando hay varios medios, es el medio menos probable para vulnerar derechos humanos. La responsabilidad de establecer esta justificación recae siempre en el estado. El principio de idoneidad requiere que las interferencia a derechos humanos autorizadas por ley son un medio efectivo para cumplir el objetivo legítimo específico identificado. El principio de proporcionalidad requiere que las decisiones que interfieran con los derechos humanos consideren la gravedad de la interferencia y otros intereses en competencia caso por caso, y sólo permitan la infracción si el interés público logra un equilibrio adecuado frente a las pérdidas de derechos humanos. Mas aún, cualquier medida que interferencia con los derechos humanos deben ser el medio menos invasivo para realmente lograr un objetivo legítimo.

Con respecto a las interferencia con el derecho a la privacidad de las comunicaciones, un estado debe establecer, como mínimo, que las siguientes condiciones existan:

1. Existe un alto grado de probabilidad que un delito serio o unaamenaza específica a un objetivo legítimo ha sido, o será, llevada a cabo;
2. Existe un alto grado de probabilidad que las pruebas pertinentes y materiales de tal amenaza específica al objetivo legítimo pueda ser obtenida mediante el acceso a la información protegida solicitada;
3. Otras, técnicas menos invasivas han sido agotadas o sería inútil, de tal manera que la técnica utilizada es la opción menos invasiva;
4. La información accesada debe limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo;
5. Cualquier exceso de información que se recaba no será retenida, pero en vez será destruida o devuelta con prontitud;
6. La información será accedida únicamente por autoridades especificadas y utilizada sólo para el propósito y duración para la que se dio la autorización; y,
7. La vigilancia de las actividades solicitadas y las técnicas propuestas no menoscaben la esencia del derecho a la privacidad o libertades fundamentales.

El cumplimiento de estas condiciones debe apreciarse con respecto a cada aspecto del

proceso de vigilancia: las decisiones para vigilar, los medios de vigilancia elegidos y los requisitos para la conservación de datos y el acceso a dichos datos.

Estos principios están profundamente arraigados en las constituciones de la región. Sin embargo, el desarrollo de las nuevas tecnologías de vigilancia y el aumento de la información que puede obtenerse por medio de la vigilancia de las comunicaciones han complicado la aplicación de estos principios, lo que resulta en algunas actividades de vigilancia gubernamental que carecen de necesidad, idoneidad o proporcionalidad.

Como ejemplo más impactante, tenemos las leyes de retención obligatoria de datos—una medida inherentemente desproporcionada. Dichas normas constituyen una seria infracción a los derechos de los usuarios de los servicios de comunicaciones al no existir una sospecha individualizada que amerite la retención de los datos de la totalidad de una población. Sin embargo, como se mencionó anteriormente, los mandatos de retención se han generalizado en muchos países de América Latina.

También hay buenas prácticas. Las leyes de vigilancia en El Salvador, Brasil, Colombia, Chile y Guatemala incorporan rigurosos análisis de necesidad, idoneidad y/o proporcionalidad, aunque queda por ver si estas leyes se aplicarán de una manera que protejan la privacidad. Algunos estados, tales como Chile y Honduras fijan límites a las operaciones de vigilancia, lo que refleja una preocupación con la proporcionalidad de la medida. La ley de Perú específicamente limita la retención de datos obtenidos por las agencias estatales para asegurar que estos se destruyan cuando ya no sean útiles para la investigacion. Algunos estados, tales como Paraguay, Uruguay, México, Colombia, Nicaragua y Chile, prohiben apropiadamente la vigilancia de ciertas comunicaciones, más comúnmente las comunicaciones entre abogado-cliente.

El Principio de Transparencia y Notificación

Los estados deberían ser transparentes sobre el uso y alcance de las leyes, reglamentos, actividades, facultades y técnicas que interfieran con los derechos humanos. Sin transparencia, la sociedad civil no puede responsabilizar a los gobiernos, y las personas que no gozan de la dignidad de saber cuando sus derechos son violados. El secreto evita que se realicen debates públicos significativos en estas materias de extrema importancia.

La transparencia es especialmente importante con respecto a la vigilancia de las comunicaciones, dado que las agencias de investigación e inteligencia tienden a considerar necesario el secreto. Desafortunadamente, estos actores comúnmente confunden la necesidad del secreto en una situación específica con una reticencia general para describir las capacidades operativas y autoridad legal que cuentan para hacer su trabajo. Incluso si la agencia posee una buena razón para mantener una investigación específica confidencial, no necesita mantener en secreto el hecho que, por ejemplo, utiliza malware y ha sido autorizado

para hacerlo como cuestión general. Sin transparencia, al público se le niega la oportunidad de debatir si el malware se debe utilizar en absoluto, y en caso afirmativo, bajo qué condiciones específicas.

Existen diversos métodos estatales que el estado (y las empresas de telecomunicaciones) pueden implementar con el fin de aumentar la transparencia en la vigilancia de las comunicaciones. Los estados pueden publicar información sobre la adquisición de tecnologías de vigilancia. Los estados pueden cumplir con las leyes de acceso a la información cuando se enfrentan a solicitudes de registros con respecto a sus leyes y capacidades de vigilancia. Los estados pueden emitir informes de transparencia con el fin de proveer información útil a los ciudadanos y usuarios, y exigir o recomendar a los proveedores de telecomunicaciones que ellos también los emitan. Las empresas de telecomunicaciones pueden establecer y publicar directrices de cumplimiento obligatorio: un conjunto de reglas que establecen las circunstancias en las que pueden o no entregar información a la policía, y los estados pueden ponerse de acuerdo para cumplir con ellos. Los estados también deberían permitir a los proveedores de informar a los usuarios que están o han sido vigilados.

Encontramos que, a diferencia de otras regiones, América Latina aún tiene que desarrollar una cultura en que las empresas de telecomunicaciones y telefonía publiquen proactivamente informes de transparencia. Varios países aún no han visto la publicación de informes de transparencia por cualquiera de las entidades estatales, empresas de telecomunicaciones o principales proveedores de aplicaciones de comunicaciones. En Nicaragua, Guatemala y Honduras, por ejemplo, ni el estado, empresas locales de comunicaciones, ni Google, Twitter o Facebook publican reportes de transparencia sobre esos países. En otros países tales como Chile, Perú, Colombia y Brasil, Google, Twitter y Facebook han publicado reportes de transparencia pero las empresas de telecomunicaciones no lo han hecho, y, en El Salvador, sólo Twitter y Facebook han publicado reportes. México es el único país donde las empresas de telecomunicaciones han publicado reportes de transparencia. Iusacell, Movistar, Nextel y Telcel han publicado reportes de transparencia a través de ANATEL (Asociación Nacional de Telecomunicaciones). Este es un paso inicial importante. Sin embargo, este reporte de transparencia sólo ofrece un número general de solicitudes realizadas por las autoridades encargadas de la persecución penal, sin proveer información detallada sobre qué tipo de solicitudes se han recibido, qué autoridades realizaron peticiones o qué razones dieron las autoridades para hacer la solicitud. En general, el secreto que rodea incluso los datos básicos sobre el alcance de la vigilancia se ha generalizado en la región. De hecho, como muchos de los regímenes de inteligencia en la región fueron formados durante las dictaduras, sigue existiendo en general el secreto por defecto en materia de vigilancia. Existen leyes secretas que autorizan la vigilancia; Sin embargo, los avances producidos en la última década en leyes de acceso a la información en toda la región deben ofrecer una oportunidad para perforar a través de estos obstáculos. Aún así, las amplias excepciones en materia de inteligencia y policía todavía existen y aún

tenemos que ver cómo se irán a aplicar las leyes en este contexto.

Nuestro estudio no encontró mejores prácticas en la región en este tema, pero algunos estados utilizan algunas buenas prácticas que vale la pena replicar con algunas mejoras. En México, las agencias gubernamentales deben divulgar periódicamente información estadística sobre la lista de peticiones que les han hecho a los proveedores de servicios de telecomunicaciones para interceptación de comunicaciones, acceso a los registros de las comunicaciones y acceso a datos de localización en tiempo real. Unos lineamientos que regula la colaboración entre gobierno y sector privado requiere a las empresas de telecomunicaciones que presenten reportes de transparencia al Instituto Federal de las Telecomunicaciones. Brasil, Chile y Colombia requieren a las agencias informen a otras agencias gubernamentales, pero no al público, al menos que el registro sea específicamente solicitada vía normas de acceso a la información pública. Los beneficios de las leyes de acceso a la información en El Salvador, Honduras, Nicaragua y Guatemala son limitados e inciertos por las ambigüedades y excepciones en esas leyes.

El Principio de Notificación requiere que los usuarios sean notificados en la mayor medida posible cuando sean vigilados. En todas las situaciones excepcionales, los usuarios deberían tener la oportunidad de impugnar la vigilancia prevista o buscar otras soluciones. Cualquier retraso en la notificación debe ser aprobado judicialmente y sólo si se prueba que la notificación pondría en grave peligro la finalidad para la que se autorizó la vigilancia o la existencia de un riesgo inminente de peligro para la vida humana. La notificación debe tener lugar cuando ya no existan esas condiciones.

El reporte identifica algunas buenas prácticas para la notificación al usuario. Perú y Chile requieren notificación a los afectados por la vigilancia, pero únicamente luego que se cerró la investigación, y con algunas excepciones. Perú permite al usuario buscar un nuevo examen judicial de la orden de vigilancia. Algunos estados, tales como Colombia y El Salvador, prevén la notificación al usuario pero sólo si el usuario es un acusado y las pruebas obtenidas por vigilancia deben ser usadas en su contra. Muchos otros estados carecen de los requisitos de notificación al usuario. De hecho, Nicaragua y El Salvador ponen el deber afirmativo de la confidencialidad a los proveedores de telecomunicaciones que les prohibe la notificación acerca de las peticiones gubernamentales de información.

Los Principios de Autoridad Judicial Competente y Debido Proceso

El principio de Autoridad Judicial requiere que la autoridad de supervisión judicial sea: (i) separada e independiente de las autoridades que restringen derechos humanos; (ii) versada en cuestiones pertinentes y competentes en la toma de decisiones judiciales; y (iii) adecuada con los recursos necesarios en el ejercicio de las funciones asignadas a la misma.

El Principio de Debido Proceso aborda muchas de las mismas preocupaciones y avances que el Principio de Autoridad Judicial Competente El debido proceso requiere que los estados respeten los derechos humanos de los individuos garantizando que los procedimientos legales que rigen cualquier interferencia con derechos humanos estén debidamente enumerados en la ley, practicados consistentemente y disponibles al público. En casos de emergencia cuando existe un riesgo inminente a la vida humana, la autorización con efecto retroactivo debe buscarse dentro de un período de tiempo razonable. La autorización con efecto retroactivo no puede justificarse únicamente por preocupaciones de riesgo de fuga o inquietudes acerca de la destrucción de evidencia.

Como resultado, la vigilancia de las comunicaciones debe ser autorizada formalmente caso por caso por una autoridad judicial independiente e imparcial, con acceso a los conocimientos tecnológicos apropiados. Esto asegura que un estado no está actuando más allá de su facultad legal y que se dé la debida consideración a los derechos humanos de los afectados por la vigilancia. Se asegura que los derechos humanos del sujeto sean protegidos en cada etapa del proceso de autorización. Al exigir que el estado justifique cada acto de vigilancia ante un juez, este principio garantiza que la vigilancia de las comunicaciones se lleve a cabo únicamente cuando la necesidad y cuando el efecto en los derechos humanos es eliminado o se reduce al mínimo. También asegura que, cuando sea posible, el sujeto de la vigilancia tenga la oportunidad de impugnar la acción deseada por el estado.

El informe nota que los prinicipios son complidos parcialmente en toda la región. Por ejemplo, las Constituciones de México y Perú requieren autorización judicial por cada interceptación de una comunicación privada, y las cortes han interpretado estos requisitos para que sean aplicados ampliamente. Pero el requisito no parece ser utilizado cuando se obtienen datos de localización. Perú permite el acceso a la localización en tiempo real sin orden de juez en casos de delitos flagrantes. Mientras que la interpretación constitucional mexicana ha considerado que los metadatos de las comunicaciones están protegidas de la misma manera que el contenido de las comunicaciones (es decir, el acceso también requiere autorización judicial previa), sin embargo, la Suprema Corte de Justicia mexicana ha determinado que no es necesario obtener autorización judicial para vigilar los datos de localización en tiempo real. En Argentina, Guatemala y Chile, la vigilancia, tanto de investigación criminal como de inteligencia, requiere aprobación judicial. En Colombia, se requiere autorización judicial previa para cualquier medida legal que afecte derechos humanos, excepto en casos de vigilancia en materia penal. En esos caso, el Fiscal General puede autorizar la vigilancia sujeta a revisión posterior. Brasil requiere aprobación judicial para la interceptación del contenido de las comunicaciones, pero no la información de los abonados.

La Suprema Corte mexicana (SCJN), en particular, ha adoptado algunas medidas positivas para garantizar la revisión judicial en los programas mexicanos de vigilancia en ciertos casos.

También ha determinado por ejemplo, que el acceso y análisis de la información almacenada en teléfono móvil sin orden judicial es una violación al derecho de inviolabilidad de las comunicaciones privadas. Del mismo modo, la SCJN recientemente ha decidido que el acceso a los metadatos de las comunicaciones almacenados por las empresas telefónicas deben tener autorización judicial previa. La misma corte ha declarado que un correo electrónico es considerado "interceptado" (de tal manera que atenta contra el derecho de inviolabilidad de las comunicaciones) en el momento que la contraseña de una cuenta ha sido tomada sin orden judicial o consentimiento del usuario, independientemente de si se analizó el contenido del correo electrónico.

El Principio de Supervisión Pública

El Principio de Supervisión Pública exige que los estados establezcan mecanismos de supervisión independientes que permitan la transparencia y rendición de cuentas de las restricciones de derechos humanos. Esta supervisión debe estar disponible al público, ya sean en forma de investigaciones públicas o, como mínimo, reportes periódicos. La supervisión pública promueve el equilibrio de poderes dentro del gobierno.

Con respecto a las infracciones a la privacidad de las comunicaciones, la supervisión pública por lo general viene en forma de supervisión judicial como se ha descrito anteriormente. Sin embargo, estos sistemas rara vez proporcionan supervisión al público que el principio requiere. En algunos sistemas jurídicos, jurados civiles y públicos supervisan y auditan el funcionamiento de diferentes operaciones gubernamentales que pueden y podrían ser implementadas para revisar los programas de vigilancia. El poder judicial también puede designar un auxiliar especial para supervisar y controlar el programa, particularmente cuando el programa está en la necesidad de una reforma significativa.

Casi no existe tradición de mecanismos de supervisión pública en la región. El Salvador, Chile, Colombia, Brasil y Argentina requieren diversas formas de auditorías, pero no se observa acceso público a ellas. La mayor parte de las agencias de inteligencia en América Latina se formaron en una época en que la división de poderes era inexistente, en otras palabras bajo el régimen militar en el que las operaciones gubernamentales fueron incorporados en el poder ejecutivo.[8] Debido a que estas agencias de inteligencia estuvieron vinculadas a las dictaduras militarizadas y la mayor parte de los gobiernos de transición hacia la democracia se produjeron mediante un proceso de negociación con la junta militar, se formaron sin controles firmes o mecanismos de supervisión. El bajo rendimiento de los mecanismos de control existentes está relacionado con la cultura de organizaciones con poco o nulo fondo democrático. Los organismos de inteligencia en América Latina se formaron en un momento en que los regímenes democráticos eran débiles, autoritarios o inexistentes.

8 José Manuel Ugarte. El control público de la actividad de inteligencia en América Latina. Ediciones CICCUS, Buenos Aires, 2012.

Por lo mismo, los mecanismos de control se situaron en la capa superior de una cultura de herencia no democrática.

Por otra parte, la marcada naturaleza del presidencialismo latinoamericano también explica por qué los mecanismo de supervisión publica son inadecuados.[9] En la región, los presidentes tienen una naturaleza más potente que, por ejemplo, su contraparte en los Estados Unidos (ellos pueden declarar emergencias, pueden introducir una legislación en el Congreso, y así sucesivamente). Por otra parte, se ha argumentado que, generalmente, la dinámica política en la región ha terminado provocando que el Congreso delegue poder en el presidente, ya sea de iure o de facto, al menos durante los momentos iniciales de su presidencia.[10] Si estos análisis son correctos, podrían explicar por qué los mecanismos de supervisión legislativa no funcionan. Las agencias de inteligencia en América Latina han sido herramientas poderosas en la política presidencial, especialmente utilizados para espiar a los grupos disidentes, políticos de oposición y periodistas independientes.[11]

Estos abusos han sido ampliamente documentados: desde los escándalos que involucran al ex-director del servicio inteligencia del Perú, Vladimiro Montesinos en los años noventa a las revelaciones sobre las escuchas telefónicas por el DAS, la agencia colombiana de inteligencia de la primera década del siglo en Colombia, hasta llegar a la conmoción más reciente relacionada con los servicios de inteligencia en la Argentina. El uso de los servicios de inteligencia para apoyar las políticas y deseos presidenciales es potente argumento para explicar por que los mecanismos de control no funcionan. La naturaleza delegativa de la política presidencial explica, por otra parte, porque mecanismos de supervisión legislativa por lo general se acercan a su tarea pasivamente, lo que es incompatible con las exigencias de las sociedades democráticas modernas.

Estas debilidades institucionales sólo pueden superarse ante la demanda de transparencia y rendición de cuentas de una sociedad civil hacia los servicios de inteligencia.

Los Principios de Integridad de las Comunicaciones y Sistemas

Estos principios buscan preservar la integridad de las infraestructuras de las comunicaciones

9 Mainwaring, Scott. "Presidentialism in Latin America." Latin American Research Review 25, no. 1, 1990: 157–179, 160.

10 O'Donnell, Guillermo A., ed. Counterpoints: Selected Essays on Authoritarianism and Democratization. First Edition edition. Notre Dame, Ind: University of Notre Dame Press, 2003.

11 Ver Ramiro Álvarez Ugarte and Emiliano Villa. El (des)control de los organismos de inteligencia en la Argentina. Asociación por los Derechos Civiles (ADC). Enero 2015. http://www.adc.org.ar/wp-content/uploads/2015/01/2015-01-23-Informe-Final-Inteligencia.pdf

al limitar la habilidad estatal de obligar a los proveedores de servicios, vendedores de hardware o software para construir capacidades de vigilar o monitorear dentro de sus sistemas, o recolectar o retener información particular con el puro fin de la vigilancia de las comunicaciones. Los principios también incorporan el derecho a los individuos de expresarse de forma anónima, mediante la preservación de la integridad de las herramientas de anonimato. Así pues, estos principios exigen a los estados de abstenerse de obligar la identificación de los usuarios, y a reconocer el derecho al utilizar el cifrado.

Desafortunadamente, amenazas a la integridad de los sistemas abundan en la región. Brasil prohíbe el anonimato en su Constitución. Colombia tiene una extrema y amplia prohibición del cifrado y, como Nicaragua y Perú, requiere a los proveedores de servicios proveer el acceso y la capacidad de interceptar para los estados deseando vigilar a sus usuarios. El Salvador obliga a los proveedores a descifrar o ser capaces de descifrar las comunicaciones sobre demanda.

El Principio del Derecho a un Recurso Efectivo

El Principio del Derecho a un Recurso Efectivo requiere que haya un recurso legal disponible para cada infracción de un derecho humano. El cumplimiento de este principio, por lo tanto, requiere que cada estado prohíba o limite la vigilancia de las comunicaciones acompañadas de una sanción contra el gobierno y la compensación de las personas afectadas.
Bueno, aunque incompleto, se encontraron ejemplos en toda la región. El principio limitante permanece con insuficiente protección de la privacidad de las comunicaciones en la primera instancia.

Por ejemplo, en Argentina y Colombia, las sanciones penales pueden ser impuestas a un miembro de los servicios de inteligencia que indebidamente intercepte o utilice comunicaciones, y que no pudo destruir los registros de las comunicaciones cuando fue requerido para ello. La legislación penal chilena sanciona a aquellos que violan el derecho a la privacidad, pero con la deficiencia en los requisitos de notificación al usuario que significa que las violaciones podrían no ser descubiertas.

Recomendaciones Finales

¿Qué sugieren hacer nuestros estudios para mejorar el estado de las leyes y prácticas de vigilancia en las Américas? Para mejorar la claridad y facilitar la comprensión del público, los estados deben tener una misma ley de vigilancia de comunicaciones en lugar de un rompecabezas de numerosas disposiciones repartidas a lo largo de las diversas leyes. Las leyes de vigilancia tampoco deben distinguir entre los diferentes tipos de datos de comunicaciones y deben ofrecer una protección igual y de la misma fuerza al contenido, “metadatos”, datos

de geolocalización, información del abonado, comunicaciones en tiempo real y datos almacenados. Y todas las infracciones al derecho de las comunicaciones privadas deben cumplir con los Principios de Necesidad y Proporcionalidad.

En varias áreas, los estados latinoamericanos mantienen prácticas favorables que pueden replicarse en toda la región. Pero, en otros casos, es necesario un cambio importante en las prácticas tradicionales. Sin embargo, estos cambios son posibles de alcanzar.

En primer lugar, necesitamos con urgencia terminar con la cultura del secreto que rodea la vigilancia de la comunicación. Necesitamos asegurar que la sociedad civil, las empresas y los responsables políticos comprendan la importancia de la transparencia en el contexto de la vigilancia, y por qué los informes de transparencia por parte de las empresas y el Estado son cruciales contra el abuso de poder.

En segundo lugar, tenemos resolver la falta de mecanismos de supervisión pública adecuados. Esa es la principal razón por la cual incluso las buenas garantías establecidas por la ley, y tenemos muchos buenos ejemplos en la región, simplemente no funcionan.

Por último, más allá de tener un diseño institucional para una mejor supervisión y control de las actividades de vigilancia, la región debe comprometerse a construir una fuerte coalición de la sociedad civil para trabajar en asegurarse que salvaguardas legales sólidas sean implentadas y ejecutadas.

Nuestra esperanza es que, a través de nuestra investigación, los estados puedan extraer de lo mejor y aprender de lo peor, que la ley latinoamericana de vigilancia tiene para ofrecer.

1.
¿Leyes o Anomia?

El Principio de Legalidad exige que cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación.

No todas las normas que limitan el derecho a la privacidad y la vigilancia de las comunicaciones son prescritas por leyes formales aprobadas por órganos legislativos. Más bien, los derechos sobre privacidad se encuentran a menudo limitados por distintos tipos de decretos administrativos, normas, y otros ejercicios del poder ejecutivo. Algunas de estas normas administrativas son adoptadas sin ningún tipo de debate público en el poder legislativo. En algunos casos, estas normas permanecen en secreto.

Las leyes de otros países son imprecisas, inconsistentes, o contienen grandes vacíos legales, y son, así, incapaces de salvaguardar las libertades fundamentales de los individuos. No tienen la suficientemente claridad acerca de los poderes de inteligencia y de los organismos del orden público, y sobre las circunstancias en las que estos organismos pueden llevar a cabo investigaciones. Generalmente, las leyes sobre vigilancia no logran especificar a qué organismo se aplica cada ley, ni quién está autorizado a vigilar. Algunas de estas leyes contienen normas sobre seguridad de datos e imponen condiciones de uso, pero no especifican quién está facultado para acceder a los datos sujetos a dichas reglas.

En otros casos, los vacíos legales son tan amplios que se puede interpretar que autorizan el uso de la gama completa de las tecnologías de vigilancia, tanto de las existentes, que incluyen el malware y los recolectores IMSI, como de cualquier tecnología de vigilancia futura. Si bien no encontramos ninguna legislación en la región que autorice expresamente el uso de ataques maliciosos o de recolectores IMSI, es un hecho conocido que su uso es ubicuo.

Lo que sigue es un listado de los ejemplos más atroces de las leyes sobre vigilancia, tanto en contextos penales como de inteligencia, que no se atienen al Principio de Legalidad.

1.1 Leyes, protocolos, y estatutos de vigilancia no están prescritos por ley

Algunas leyes, protocolos, lineamientos y reglamentos sobre la vigilancia de las comunicaciones se mantienen secretos, y las instalaciones secretas de tecnología de vigilancia

se colocan bajo la autoridad de dichas normativas. Dichas autorizaciones de vigilancia secretas permiten un espionaje sin control. Este es un patrón de comportamiento que hemos identificado en varios países en el mundo. Adicionalmente, los organismos de aplicación de la ley y los gobiernos abusan de las nuevas tecnologías y adquieren capacidades de vigilancia más invasivas, y adoptan procedimientos secretos para emplearlas.

Hallamos normativas secretas en El Salvador, Uruguay, y Perú.

EL SALVADOR: El artículo 31 de la Ley Especial para la Intervención de Telecomunicaciones establece los casos en los que se autoriza la intervención de las comunicaciones. Este artículo indica que, entre otras cosas, el Fiscal General debe elaborar normativas públicas y reglamentos que regulen las operaciones policiales (en las que se encuentra comprendida la vigilancia de las comunicaciones), así como también un proceso para la selección y fiscalización del director, funcionarios, personal y miembros de la Policía Civil Nacional.[12] La reglamentación y las normativas específicas de esta ley son "confidenciales", según la Unidad de Acceso a la Información Pública de la Fiscalía General, conforme a una petición en relación con la Ley de Acceso a la Información.[13] Por el momento, las personas de El Salvador no tienen manera de saber cómo y por qué están bajo vigilancia o cómo está supervisada esa vigilancia.

URUGUAY: El gobierno adquirió *El Guardián* de manera secreta, un sistema electrónico de vigilancia creado por la compañía brasilera Digitro Technology Ltda, cuyo uso todavía no está regulado a través de normativas públicas.[14] Según la prensa uruguaya, el Ministerio de Economía emitió un decreto secreto que explicaba la necesidad del gobierno de adquirir tecnología de vigilancia y brindó incentivos tributarios a aquellas compañías de telecomunicaciones que pudieran proporcionarle dicha tecnología al Ministerio del Interior. El periódico *El Observador* reveló que el gobierno también elaboró un protocolo de colaboración secreta entre el Ministerio del Interior y las compañías de telecomunicaciones

12 El Salvador, Ley Especial para la Intervención de las Telecomunicaciones, Asamblea Legislativa, (2010). http://www.oas.org/juridico/PDFs/mesicic4_slv_telecom.pdf

13 Resolución 128-UAIP-FGR-2015. Petición de acceso a la información presentada por Marlón Hernández, investigador de Fundación Acceso, Costa Rica. Citada previamente en: Fundación Acceso (coord. por Luciana Peri), ¿Privacidad Digital para Defensores y Defensoras de Derechos?: un Estudio Sobre Cómo los Marcos Legales de El Salvador, Guatemala, Honduras y Nicaragua Pueden ser Utilizados Para la Protección, Criminalización y/o Vigilancia Digital de Defensoras y Defensores de Derechos Humanos, (2015). https://necessaryandproportionate.org/files/2016/05/16/investigacion-privacidad-digital-fa.pdf

14 Para una investigación más pormenorizada, lea a Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay", Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/uruguay

locales, que regulaba el uso de *El Guardián*.[15] Este documento establecía la obligación de las compañías de telecomunicaciones de conectar sus computadoras a *El Guardián*.[16] Permanece en secreto la información sobre la compra y la regulación de este sistema de vigilancia electrónico.

PERÚ: El protocolo de acceso a datos de geolocalización se ha mantenido en secreto. En octubre de 2015, bajo la Resolución Ministerial 0631-2015-IN, el Ministerio del Interior, con la autorización del Decreto Legislativo 1182, aprobó un protocolo que regula el acceso a los datos de geolocalización de teléfonos móviles y otros dispositivos electrónicos. Sobre la base de la excepción relacionada con la seguridad nacional que contiene la Ley de Libertad de Información, el Ministerio clasificó este protocolo como "información reservada".[17] Así, los ciudadanos peruanos quedaron inhabilitados para obtener información acerca del protocolo, aun cuando es a ellos a quienes se les aplica el procedimiento. Esto es especialmente sorprendente porque un protocolo diferente, el Protocolo de Intervención y Grabación de Comunicaciones, que fue aprobado en noviembre de 2014 por Resolución Ministerial Nº 0243-2014-JUS, es público.

1.2 Las órdenes de retención de datos carecen de autorización legislativa

Los siguientes países han aprobado obligaciones de retención de datos que no están prescritas por ley, sino por una autoridad ejecutiva o administrativa.

BRASIL: Se establecieron varias obligaciones de retención de datos mediante resoluciones administrativas emitidas por ANATEL, el regulador de telecomunicaciones brasilero, y no mediante la adopción de una ley formal. Por ejemplo, la Resolución de ANATEL 426/05 exige a los proveedores de servicios retener los registros telefónicos y otros datos procesados por los proveedores de servicio de telefonía fija. La Resolución de ANATEL 477/07 obliga a los proveedores de servicios de telefonía móvil a retener los documentos de facturación que contengan datos sobre las llamadas entrantes y salientes de sus suscriptores por al menos cinco años. Estos datos comprenden hora, duración, y precio de las llamadas, así como también la información de cuenta de los suscriptores. Asimismo, la Resolución de

15 Leonardo Pereyra, "El Guardián espiará desde enero mails y celulares", *El Observador*, 12 de Octubre, (2014). http://www.elobservador.com.uy/el-guardian-espiara-enero-mails-y-celulares-n289757

16 Leonardo Pereyra, "El Guardián espiará desde enero mails y celulares", *El Observador*, (2014). http://www.elobservador.com.uy/el-guardian-espiara-enero-mails-y-celulares-n289757

17 La ONG Hiperderecho presentó una petición de libertad de información, la cual fue rechazada en su momento. Para un análisis más detallado, lea a Miguel Morachimo, "Perú: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Perú", Electronic Frontier Foundation & Hiperderecho, (2016). https://necessaryandproportionate.org/country-reports/peru

ANATEL 614/13 también obliga a los proveedores de servicio de Internet a retener los registros de conexión y la información de la cuenta del suscriptor relativa a las conexiones a Internet por al menos un año.[18]

COLOMBIA: En el contexto penal, el Decreto 1704 de 2012 establece varias medidas de vigilancia que vulneran los derechos humanos, como la obligación de retención de datos para los servicios de telecomunicaciones (Proveedores de Servicios de Internet) y proveedores de servicios de redes. Fue una agencia administrativa — el Ministerio de Tecnologías de la Información y las Comunicaciones — y no la legislatura quien adoptó este decreto.

PERÚ: El poder ejecutivo emitió el Decreto Legislativo 1182 (también conocido como Ley Stalker) el día previo al Día de la Independencia de Perú, momento en que la mayoría de los sectores comerciales estaban cerrados. El Decreto Legislativo 1182 obliga a los concesionarios de servicios públicos de telecomunicaciones y a las entidades públicas que prestan servicios de telecomunicación (como los aeropuertos que brindan Wi-fi) a llevar a cabo una retención de datos obligatoria.[19]

HONDURAS: En virtud de la resolución administrativa RN 004/11, la cual aprobó la normativa para los proveedores de servicios en Honduras, los operadores del Servicio de Internet o Acceso a Redes Informáticas, quedan obligados a retener las "direcciones IP utilizadas por los usuarios del servicio, que sirvan como fuente para investigación judicial o de las autoridades correspondientes por un año solamente". Esta resolución fue emitida por CONATEL, el regulador de telecomunicaciones del país.[20]

En cambio, la obligación de retención de datos en México se adoptó a través de un acto legislativo que entró en vigencia en 2009 en lo que se conoce actualmente como la derogada Ley Federal de Telecomunicaciones y Radiodifusión (LFTR); la nueva LFTR establece el plazo de retención de datos a 24 meses.

En Brasil, existen dos disposiciones legales adicionales que crean obligaciones de retención de datos: la Ley 12.850 de 2003 exige a los proveedores de servicios de telefonía fija y móvil retener los registros de llamadas por un periodo de cinco años, y el Marco Civil que obliga a los "sistemas autónomos" que proveen Internet a retener los registros de conexión por un

18 A los efectos de este reporte, "nformación de la cuenta del suscriptor" hace referencia a la información contenida en los registros del usuario en la compañía telefónica, operador de sistema autónomo, o proveedor de aplicación.

19 Código Procesal Penal de Perú, art. 259. http://spij.minjus.gob.pe/CLP/contenidos.dll?f=templates&fn=default-nuevocodprocpenal.htm&vid=Ciclope:CLPdemo

20 Honduras, Resolución NR004/11, Comisión Nacional de Telecomunicaciones, CONATEL, (2011). http://www.tsc.gob.hn/leyes/Reglamento%20del%20Servicio%20de%20Internet%20o%20Acceso%20a%20Redes%20Inform%C3%A1ticas.pdf

año. Conozca más sobre la retención de datos en la sección 1.3.2.

1.3 Los marcos legales amplios o imprecisos son propensos al abuso

Hemos hallado en toda la región varias leyes de vigilancia que contienen grandes vacíos legales o cuya redacción es imprecisa e incoherente. Son, así, incapaces de salvaguardar las libertades fundamentales de los individuos. Muchas de estas no aclaran la idoneidad de los pedidos de vigilancia, las personas que pueden acceder a los datos, ni las circunstancias y condiciones bajo las cuales pueden hacerlo.

1.3.1 Rastreo de ubicación

Hoy en día, la mayoría de las personas camina con un dispositivo que transmite su ubicación. Los teléfonos celulares se registran a una torre cercana mientras la persona se mueve de un lugar a otro. La compañía telefónica puede recoger esos datos en tiempo real o de manera retroactiva para ubicar el teléfono físicamente con un grado de precisión variable. Las compañías también pueden determinar a los dueños de cada aparato dentro de un rango determinado en relación con una torre determinada. Los teléfonos que tienen el GPS habilitado brindan una ubicación mucho más precisa. En EFF, afirmamos que la ley debe proteger la información de ubicación exigiendo que la policía obtenga una orden judicial antes de recolectar datos sensibles. También trabajamos para asegurarnos que los proveedores de servicios basados en la ubicación no abusen de la información que recopilan ni la entreguen a la policía sin contar con garantías legales convincentes.

Si bien los individuos pueden no darse cuenta de las implicaciones ligadas al monitoreo constante de sus ubicaciones, esta información puede ser extremadamente sensible, ya que tiende a revelar relaciones personales (como las identidades de aquellos que viven o pasan la noche juntos), prácticas religiosas, amistades y afiliaciones, consultas médicas, participación en organizaciones y eventos políticos, y muchas otras relaciones y actividades de la vida diaria.

Aunque algunos de los datos mencionados se pueden averiguar por otros medios, el seguimiento de la ubicación puede revelar datos muy sensibles de manera sistemática y a gran escala; imaginemos como ejemplo la creación de un registro con todo los teléfonos celulares presentes en una manifestación política o en una protesta.

PERÚ: Este país no brinda una firme protección legal para la privacidad de la ubicación. El Decreto Legislativo 1182 concede a la policía nacional acceso ilimitado y sin orden de judicial a los datos de ubicación en tiempo real de los teléfonos celulares o dispositivos electrónicos en casos penales, siempre y cuando ocurran simultáneamente los siguientes tres requisitos: (i) cuando se trate de flagrante delito, (ii) cuando el delito investigado sea sancionado con

pena superior a los cuatro años de privación de la libertad, y (iii) cuando el acceso a los datos constituya un medio necesario para la investigación.[21] El artículo 259 del Código Procesal Penal define el concepto de "flagrante delito" de manera muy amplia. Esta definición incluye procedimientos de emergencia (cuando existe un riesgo inminente para la vida humana), también incluye cualquier delito que se esté cometiendo en el momento o que acabe de cometerse, hasta 24 horas después de su comisión.[22] El Decreto Legislativo 1182 tampoco logra definir a los datos de ubicación o geolocalización, ni delimita las entidades obligadas a implementar esta obligación. No sólo obliga a los proveedores de telecomunicaciones sino también a cualquier entidad pública o privada que de acceso a Internet a retener los datos de ubicación de los usuarios. Además, las mismas entidades quedan obligadas a desarrollar y brindar a la Policía Nacional un "acceso exclusivo" a estos datos.[23]

COLOMBIA: El Decreto 1704 de 2012 exige a los servicios de telecomunicaciones (Claro y Movistar) y a los proveedores de redes que entreguen los datos de ubicación a las autoridades. Tales datos incluyen las coordenadas geográficas, la potencia de la señal, y "otros datos" que ayudan a determinar la ubicación geográfica de la terminal, el equipo o el dispositivo. Los datos de ubicación deben ser entregados en tiempo real o en línea a solicitud del Ministerio Público. Los proveedores de contenidos y de aplicaciones de Internet (Mercadolibre.com y Tappsi.com) quedan fuera de esta disposición.

Las disposiciones sobre el rastreo de la ubicación en tiempo real incluidas en el artículo 4 no dejan en claro qué tipo de datos deberán ser entregados en tiempo real a la Fiscalía General de la Nación. Los datos por suministrar, según este artículo, incluyen "la información específica contenida en las bases de datos de las compañías, tal como sectores, coordenadas geográficas y potencia, entre otras". El uso de "entre otras" y "tal como" hace posible que estas compañías entreguen a las autoridades información inespecífica.

MEXICO: La nueva Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) carece de claridad con respecto a cuáles son las autoridades que pueden acceder a los datos de geolocalización. El artículo 190, sección I de la LFTR obliga a las compañías de telecomunicaciones a "colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil".

---

21 Código Procesal Penal de Perú, art. 259. http://spij.minjus.gob.pe/CLP/contenidos.dll?f=templates&fn=default-nuevocodprocpenal.htm&vid=Ciclope:CLPdemo

22 Para un análisis detallado de los problemas legales relacionados con el rastreo de la ubicación, lea a Miguel Morachimo, "Perú: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Perú", *Electronic Frontier Foundation & Hiperderecho*, (2016).

23 Decreto Legislativo 1.182 de Perú, art. 4, y Disposiciones Complementarias Finales, artículo primero.

Esta disposición concede poder a "autoridades que no tenían, ni tienen esta facultad en una ley habilitante, como las "agencias de seguridad" o las "instancias de administración de justicia", que no se encuentran definidas ni en la LFTR ni en ninguna otra ley".[24] Sin embargo, una resolución judicial de la Suprema Corte de México en 2016[25] estableció que las únicas autoridades facultadas para acceder a los datos de ubicación son los fiscales federales y estatales, la Policía Federal, y el Centro de Investigación y Seguridad Nacional (CISEN).[26]

1.3.2 Obligaciones de retención de datos

BRASIL, COLOMBIA, CHILE, MÉXICO, PERÚ, y HONDURAS poseen obligaciones de retención de datos que exigen a ciertas compañías tecnológicas a registrar grandes cantidades de datos invasivos sobre los usuarios y proveer el acceso a esta base de datos a las autoridades a petición de estas, en aplicación de la ley. Las obligaciones de retención de datos impuestas por el Gobierno afectan a millones de usuarios comunes y es, por naturaleza, una medida desproporcionada.

La retención de datos compromete el anonimato en línea, que es esencial para los informantes, investigadores, periodistas, y aquellos que están involucrados en algún tipo de expresión política. También incluye la privacidad de ciertas comunicaciones protegidas. Estas pueden darse en las comunicaciones entre abogado-cliente, médico-paciente, y periodista-fuente.

Las obligaciones de retención de datos exigen a los proveedores de servicios de Internet (PSI) y a las compañías de telecomunicaciones a crear grandes bases de datos de información sobre las comunicaciones de los usuarios. Debido a que estas bases de datos son vulnerables al robo y a la divulgación accidental, estas obligaciones en realidad aumentan los riesgos para la privacidad.

Los marcos legales para la retención de datos obligatoria, que por lo general traen aparejadas disposiciones legales que permiten a investigadores tener acceso a esos datos, son imprecisos sobre el tipo de datos que deben retener las compañías, las personas autorizadas para acceder a ellos y los propósitos de ese acceso.

América Latina se ha convertido en un serio transgresor del derecho a la privacidad al implementar estas peligrosas obligaciones. Paraguay es el único país de la región que rechazó

24 Para un análisis detallado sobre los problemas legales relacionados con la retención de datos, *lea a* Luis Fernando García, "México: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México", *Electronic Frontier Foundation & InternetLab*, (2016). https://necessaryandproportionate.org/country-reports/mexico

25 Segunda Sala, Suprema Corte, Amparo en Revisión 964/2015.

26 Luis Fernando García, "México: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México", *Electronic Frontier Foundation & InternetLab* (2016). https://necessaryandproportionate.org/country-reports/mexico

un proyecto de ley de retención de datos obligatoria. Este rechazo estuvo alineado con la sentencia de la Gran Sala del Tribunal de Justicia de la Unión Europea que invalidó en 2014 la Directiva sobre la Retención de Datos por vulnerar gravemente el derecho a la privacidad.[27]

HONDURAS: La obligación de retención de datos que establece el artículo 20 del Reglamento del Servicio de Internet o Acceso a Redes Informáticas (Resolución NR004/11) no indica qué entidades pueden tener acceso a los datos retenidos. La Resolución de CONATEL establecía que los proveedores de servicios tenían la obligación de retener las direcciones IP por un año para que sirva como fuente de "investigación judicial" o de otras investigaciones sobre actividades ilícitas de "autoridades competentes", "cuando corresponda". Esta resolución no logra especificar los estándares para el acceso a los datos ni ninguna otra limitación con respecto a los tipos de crímenes por los cuales se pueden extraer esos datos. También amplía el propósito de extraer datos en instancias diferentes de las investigaciones judiciales.

COLOMBIA: En el contexto penal, El Decreto 1704 de 2012 impuso una obligación de retención de datos para los servicios de telecomunicaciones, como los Proveedores de Servicio de Internet y proveedores de redes,[28] para conservar de manera actualizada "la información de los suscriptores" por un periodo de cinco años, y deben brindar esta información a la fiscalía general cuando ésta lo solicite.[29]

Esta obligación de retención de datos brinda ejemplos de los tipos de datos que deben retener los servicios de telecomunicaciones y los proveedores de redes. Esta información consta de los "datos del suscriptor, 'tales como' la identidad, dirección de facturación y tipo de conexión". No obstante, el uso de la frase "tales como" pone en evidencia que esta lista no es exhaustiva; este carácter indefinido de la lista crea ambigüedad en lo que respecta a los demás datos del suscriptor que pueden retenerse de manera legal.

El artículo tampoco es claro con respecto a cuáles son las autoridades que pueden acceder a esos datos y bajo qué condiciones. En un principio, el decreto indicaba que la Fiscalía de la Nación u "otras autoridades competentes" (por ejemplo, la Dirección de Impuestos y Aduanas Nacionales y la Contraloría General de la República) podían acceder a los datos mediante la policía judicial a cargo de la investigación del caso. Sin embargo, esta generalización no consigue identificar específicamente quiénes eran dichas autoridades. A

27 Tribunal de Justicia de la Unión Europea, Sentencia en las causas acumuladas C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger et al.* http://curia.europa.eu/juris/documents.jsf?num=C-293/12

28 En el marco legal colombiano, las compañías de Internet y las aplicaciones de Internet se consideran proveedores de contenido y de aplicaciones, y, por lo tanto, quedan excluidas del Decreto 1704. *Vea* la Resolución 000202 (2010).

29 Colombia, Decreto 1.704 de 2012, art. 4.

raíz de la demanda que interpuso un ciudadano, se derogó la frase "otras autoridades competentes". Ese vacío legal fue resuelto por una decisión del Consejo de Estado en 2016.[30]

Actualmente ha quedado aclarado que es únicamente la Fiscalía de la Nación quien está autorizada para acceder a los datos retenidos, mediante los organismos de la policía judicial.

En el contexto de inteligencia y contrainteligencia, la Ley 1.621 de 2013 plantea problemas similares. El artículo 44 de la Ley 1.621 obliga a los operadores de servicios de telecomunicaciones a suministrar a los organismos de inteligencia y contrainteligencia "el historial de comunicaciones" - los datos técnicos de identificación de los suscriptores y la localización de las celdas – junto con "cualquier otra información" que contribuya a la localización de los suscriptores.

Se suministra esta información con la condición que lo solicite una agencia de inteligencia, y durante el desarrollo de una "operación autorizada", siempre que sea técnicamente viable. Las agencias de inteligencia limitarán la información solicitada a un máximo de cinco años. Esto implica que esta disposición no impone de manera expresa la obligación de retención de datos para todas las compañías, sino solo para aquellas que ya tienen los datos.[31]

Sin embargo, las compañías de telefonía móvil y los proveedores de redes, incluyendo a los proveedores de servicios de Internet, se ven obligados de antemano a retener datos, según el Decreto 1704 de 2012.

La ley establece que los proveedores de redes y servicios de telecomunicaciones no se hacen responsables, bajo ninguna circunstancia, de lo que las agencias de inteligencia y contrainteligencia hagan con los datos, de conformidad con lo que dicta esta ley.[32]

MÉXICO: El artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) de 2014 ordenaba a los proveedores de telecomunicaciones a retener datos por 12 meses en sistemas que permitieran a las agencias de aplicación de la ley acceder y obtener la información de manera electrónica y en tiempo real. Después de este periodo de un año, los proveedores de telecomunicaciones debían conservar esos datos por 12 meses más, y cuando así se les solicite, entregarlos a las autoridades dentro de las siguientes 48 horas. La Corte Suprema de México declaró recientemente que esta ley es constitucional, afirmando que la

30 "Tumban polémico decreto sobre acceso a datos privados", *Semana Económica,* (2016). http://www.semana.com/nacion/articulo/consejo-de-estado-solo-la-fiscalia-podra-tener-acceso-a-datos-privados/465546

31 Juan Camilo Rivera y Katitza Rodríguez, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Colombia," *Comisión Colombiana de Juristas, Electronic Frontier Foundation, & Fundación Karisma,* (2016). https://necessaryandproportionate.org/country-reports/colombia

32 Ley 1.621 de 2013, art. 44.

obligación de retención de datos no representa una vulneración del derecho a la inviolabilidad de las comunicaciones.[33]

A diferencia de otros países, la obligación de retención de datos impuesta por México sí brinda una lista exhaustiva (aunque muy amplia) de los datos que deben retener las compañías de telecomunicaciones:

a) Nombre, denominación o razón social y domicilio del suscriptor;

b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e) La fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda);

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h) La obligación de conservación de datos comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

El lenguaje utilizado en el artículo 190, sección III de la LFTR es altamente ambiguo en cuanto a las autoridades que están facultadas para acceder a los datos retenidos. Este artículo autoriza la entrega de los datos retenidos a "las autoridades a las que se refiere el artículo 189 de esta Ley que así lo requieran". El artículo 189 de la LFTR crea la obligación de las compañías de telecomunicaciones y proveedores de servicios en línea, de aplicaciones y de contenidos, de atender "todo mandamiento por escrito, fundado y motivado de la autoridad competente", y se menciona, entre otros, a las "instancias de seguridad y procuración de justicia" sin establecer de manera clara cuáles son las autoridades que entran en esas categorías:[34]

33 Segunda Sala, Suprema Corte, Amparo en Revisión 964/2015.

34 Luis Fernando García, "México: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México", *Electronic Frontier Foundation & InternetLab*

> *Muchas autoridades consideran que el artículo 189 de la LFTR les da poder suficiente como para usar herramientas de vigilancia encubierta y que este poder no necesita quedar detallado en ninguna otra norma. Por ejemplo, la "Unidad de Inteligencia Financiera" de la Secretaría de Hacienda y Crédito Público entra en la categoría de "instancia de seguridad" según el artículo 189 y un documento que no es una ley formal y material, conocido como la "Guía de Colaboración".*[35] *[...] Además, existen reportes que afirman que autoridades como el Instituto Nacional Electoral pueden haber enviado este tipo de pedido con el objetivo de acceder a los datos personales de usuarios de servicios de telecomunicaciones.*[36]

Hace poco, la Suprema Corte de México[37] solucionó este problema al resolver que las únicas autoridades facultadas para acceder a los datos retenidos son los Fiscales Federales y Estatales, la Policía Federal y el Centro de Investigación y Seguridad Nacional (CISEN).[38]

CHILE: El artículo 222 del Código Procesal Penal de este país indica que los proveedores de telecomunicaciones deben almacenar una lista de las direcciones IP de los suscriptores y los registros de conexión por un año, y mantener esos datos a disposición del Ministerio Público. Los proveedores que se rehúsen a cooperar serán sancionados.

El "Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de comunicaciones" no requiere autorización judicial. En cambio, exige que la información retenida esté disponible para cualquier fiscal y cualquier institución que esté autorizada a solicitarla, sin necesidad de contar con una autorización judicial por cada interceptación o solicitud.

ARGENTINA: En la resolución de *Halabi* en 2009, la Corte Suprema declaró inconstitucional una ley que buscaba brindar al gobierno fácil acceso a los registros de telecomunicaciones y retenía los datos de la población entera. En febrero de 2004, la Ley 25.873 modificó la Ley de Telecomunicaciones de 1972. Esta ley exige que todos los prestadores de servicios de telecomunicaciones dispongan de los recursos tecnológicos y humanos que permitan la observación remota de las comunicaciones a solicitud del Poder Judicial o el Ministerio Público (artículo 1). También establece que los prestadores deben

(2016). https://necessaryandproportionate.org/country-reports/mexico

35 Acuerdo 016/2014 por el que el Titular de la Unidad de Inteligencia Financiera designa a los servidores públicos que se mencionan en el documento, para efectos de lo dispuesto en el artículo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión, en el Diario Oficial de la Federación, art. 189, (2014).

36 Christine Murray y Joanna Zuckerman Bernstein, "Mexico Ramps up Surveillance to Fight Crime, but Controls Lax, *Reuters*, (2015). http://www.reuters.com/article/2015/10/12/us-mexico-surveillance-idUSKCN0S61WY20151012

37 Suprema Corte. Segunda Sala. Amparo en Revisión 964/2015.

38 Luis Fernando García, "México: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México", *Electronic Frontier Foundation & InternetLab* (2016). https://necessaryandproportionate.org/country-reports/mexico

crear un registro de usuarios que incluya información sobre el tráfico de sus comunicaciones por un plazo de diez años.

La presidencia suspendió la ley a través del Decreto 357/05, después de haber enfrentado duras críticas mediáticas.[39]

El artículo 8 de la Resolución 5/2013 obliga a todos los prestadores de servicios de telecomunicaciones a conservar todos los datos recopilados a través de sus sistemas electrónicos por al menos tres años únicamente para que sirvan de indicadores de calidad. Sin embargo, según este artículo, las autoridades de aplicación pueden requerir "la entrega total o parcial de los mismos y proceder a su almacenamiento durante el lapso que considere necesario".[40] También, para asegurar calidad en el servicio, los prestadores de telecomunicaciones deben brindar a las autoridades de aplicación "el libre acceso a sus redes y a su información".[41] Finalmente, el Ente Nacional de Comunicaciones (ENACOM), con el propósito de satisfacer los requisitos de calidad, podrá "requerir a los prestadores de servicios de telecomunicaciones la información que estime pertinente".[42]

Todas estas medidas resultan desproporcionadas, ya que conceden a ENACOM acceso a los datos de los usuarios bajo la premisa general de "calidad". Más aún, no existen protecciones vigentes para la prevención de las acciones abusivas llevadas a cabo por dichas autoridades.[43]

PARAGUAY: El regulador de telecomunicaciones CONATEL emitió una resolución que obliga a las compañías a retener datos relacionados con llamadas telefónicas y mensajes de texto por un periodo de seis meses, por motivos de comercio electrónico. Prohíbe expresamente el acceso a estos datos por razones que no fueran esa.

PERÚ: El Decreto 1182 obliga a los PSI locales y a las compañías telefónicas a retener los detalles de las comunicaciones y la ubicación de todos los ciudadanos peruanos por un periodo de tres años. Los datos retenidos podrían quedar a disposición de las autoridades de

---

39 Beatriz Busaniche, Noticia de Último Momento sobre Retención Obligatoria de Datos Personales, Electronic Frontier Foundation, https://www.eff.org/node/81911

40 Ministerio de Planificación Federal, Inversión Pública y Servicios, Secretaría de Comunicaciones, Resolución 5/2013, (2013). http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

41 Ministerio de Planificación Federal, Inversión Pública y Servicios, Secretaría de Comunicaciones, Resolución 5/2013, art. 5, sección 2, (2013), http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

42 Ministerio de Planificación Federal, Inversión Pública y Servicios, Secretaría de Comunicaciones, Resolución 5/2013, art. 3, (2013). http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

43 Verónica Ferrari y Daniela Schnidrig, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina", (2015). https://necessaryandproportionate.org/country-reports/argentina

aplicación de la ley mediante una orden judicial por posible uso futuro.

Los ciudadanos de Perú apodaron este decreto como #Leystalker, con el propósito de evocar una imagen de alguien que usa la tecnología para espiar los movimientos diarios de una persona en línea. El decreto es bastante general con respecto a las entidades que se ven obligadas a retener datos. Incluía no solo a los PSI grandes y pequeños, sino también cualquier entidad pública que brinde acceso a Internet a un consumidor final, como las escuelas públicas, bibliotecas públicas, aeropuertos, y otras entidades gubernamentales. El decreto no delimita el tipo de datos por registrar, las limitaciones para el acceso a estos ni las condiciones de uso, así como tampoco especifica las reglas de seguridad de datos aplicables.

BRASIL: Este es el único país de la región que ha desarrollado reglas distintas en relación con la retención de datos dependiendo del tipo de servicio: línea de telefonía fija, móvil o servicios de Internet.

El artículo 22 del Reglamento del Servicio de Telefonía Fija (Resolución de ANATEL 426/05) establece que las compañías de telecomunicaciones deben retener los datos relacionados con la provisión de servicios, incluyendo los registros de llamadas, por al menos cinco años. Este artículo no describe el tipo de datos por retener, ni quién puede acceder a ellos, ni los propósitos de tal acceso.

Del mismo modo, el Reglamento del Servicio Móvil Personal (Resolución de ANATEL 477/07) exige a los proveedores de telecomunicaciones que mantengan "a disposición de la ANATEL y demás interesados, los documentos de naturaleza fiscal que contengan datos sobre las llamadas entrantes y salientes, la fecha, hora, duración y precio, así como también la información de la cuenta de los suscriptores [...]" por al menos cinco años. Deben mantener esta información a disposición de la Agencia Nacional de Telecomunicaciones y otros interesados:

> *Esta ley exige que las entidades legales retengan y conserven los documentos de facturación a disposición de la Secretaría de Ingresos Federales de Brasil, por un periodo delimitado en la legislación fiscal para llevar disputas ante la corte (prazo decadencial), que es de cinco años. Los artículos 42 y 58 también establecen "el mínimo de información personal" que los usuarios deben brindar para poder adquirir el servicio de telefonía móvil (nombre, número de identificación, y número de identificación fiscal). En la práctica, esto significa que se necesita un número de contribuyente fiscal para poder adquirir el servicio, lo que compromete el anonimato.*
>
> *La justificación del plazo de cinco años para la obligación de retención de datos de los servicios de telefonía, y la razón de fiscalización y supervisión de los documentos de facturación que realiza ANATEL están detalladas en el artículo 10, XXII de la*

Resolução No. 477/07.

Sin embargo, ambas reglas, que imponen las obligaciones de retención de datos a los servicios de telefonía móvil y fija han dado lugar a un almacenamiento de registros que es conveniente para las actividades de fiscalización e investigación del Estado.

La Ley 12.850/13 [Ley de Crimen Organizado], que obliga a las compañías telefónicas a retener los datos específicamente con esos fines, data de 2013. Además, las disposiciones de estas resoluções establecen obligaciones de retención de datos incluso para los servicios que proveen planes de tarifa única, en los que la duración de la llamada o el número marcado no afectan el precio que paga el usuario. Es por eso por lo que es razonable suponer que las regulaciones de ANATEL sobre retención de datos van mucho más allá de los propósitos asociados con sus responsabilidades.[44]

El artículo 53 del Reglamento del Servicio de Comunicación Multimedia (Resolución de ANATEL 614/13) exige que los prestadores de servicios de Internet retengan los registros de los suscriptores y los datos de la cuenta por un año:

[L]a definición de registros de conexión se encuentra en el artículo 4, XVII (el conjunto de datos referidos a la fecha y hora de una conexión a Internet, con una dirección IP determinada en la terminal para paquetes de datos entrantes y salientes, entre otros datos que permitan la identificación de la terminal usada para el acceso). Este periodo de retención más corto en comparación con las obligaciones de retención de datos de los servicios de telefonía, así como también la clara descripción de los datos por retener, puede atribuirse a que la regulación fue elaborada mientras se llevaban a cabo debates sobre la Ley No. 12.965/14 (Marco Civil da Internet) y a la publicidad relativa a las decisiones internacionales en contra de la retención de datos, las cuales recibieron atención especial por parte de la comunidad académica y la sociedad civil.[45]

Muchas interpretaciones de la Ley de Crimen Organizado 12.850 de 2013 provocaron confusión y resultaron en la retención de registros de compañías telefónicas con el propósito de identificar a una persona sometida a una investigación penal.[46]

---

44 Para un análisis detallado sobre los problemas legales relacionados con la retención de datos, *lea a* Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab* (2015). https://necessaryandproportionate.org/country-reports/brazil

45 Para un análisis detallado sobre los problemas legales relacionados con la retención de datos, *lea a* Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab* (2015). https://necessaryandproportionate.org/country-reports/brazil

El artículo 17 de la Ley 12.850 de 2003 exige a los proveedores de telefonía fija y móvil retener los registros de llamadas (*registros de identificação*) de origen y de destino, nacionales e internacionales, por un periodo de cinco años, y mantener dichos registros a disposición del Jefe de la Policía Civil y del Ministerio Público. Si bien esta obligación se encuentra en una ley cuyo objetivo es combatir las organizaciones criminales, dicha ley no contiene una disposición que limite el uso de los datos retenidos para otros tipos de actividades delictivas. Esta regulación no especifica el tipo de datos que serán registrados ni las limitaciones para el acceso a estos ni las condiciones de uso, así como tampoco determina las reglas de seguridad para proteger los datos. La norma indica que el Jefe de la Policía Civil y el Procurador General pueden acceder a la información de la cuenta del acusado sin necesidad de contar con una orden judicial. Actualmente se está impugnando la constitucionalidad de esta disposición mediante una *Ação Direta de Inconstitucionalidade*, ADI 5063/DF, que está en espera de juicio.[47]

El artículo 15 de la misma ley habilita al Jefe de la Policía Civil y al Ministerio Público a obtener los datos de registro del acusado (*dados cadastrais*) sin contar con una orden judicial, con el objeto de "conseguir información que informe exclusivamente su cualificación personal, familiar, y las direcciones almacenadas por los tribunales electorales, compañías telefónicas, instituciones financieras, proveedores de Internet, y administradores de tarjetas de crédito".[48]

El artículo 21 penaliza rehusarse a brindar "información de la cuenta (*dados cadastrais*), registros, documentos, y la información que requiera el juez, el Ministerio Público o el delegado de la Policía Civil durante las actividades de una investigación o proceso", y establece sanciones que van desde seis meses hasta dos años de privación de la libertad, y multa. Según los autores del reporte "Vigilancia Estatal de las Comunicaciones en Brasil y la Protección de los Derechos Fundamentales", estas autoridades, sin contar con órdenes judiciales, han exigido a las compañías los registros telefónicos y los datos de ubicación, bajo amenaza de sanción.[49]

---

46 Extracto del reporte de Brasil, Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Brasil", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

47 Extracto del reporte de Brasil, Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab* (October, 2015). https://necessaryandproportionate.org/country-reports/brazil

48 Ley de Organización Criminal 12.850 de 2013, art. 15. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

49 Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

El artículo 13 del Marco Civil sólo requiere que los operadores de "sistemas autónomos" que presten servicios de acceso a Internet retengan los registros de conexión por un año. En este caso, un "sistema autónomo" es un término técnico que hace referencia a aquellos que administran bloques de direcciones IP y sus correspondientes sistemas autónomos con propósitos de enrutamiento. Esto quiere decir que la obligación de retener aplica sólo a los grandes proveedores de servicios de Internet y no a cada entidad que brinde acceso a Internet para consumidores finales, como escuelas, bibliotecas, cibercafés, o proveedores de Internet pequeños y locales que no administren sus propios bloques de direcciones IP.

El artículo 15 solicita que los operadores comerciales de "aplicaciones" de Internet retengan los registros correspondientes al acceso a sus propias aplicaciones por un periodo de seis meses. También se les puede ordenar a los operadores de tales aplicaciones sin carácter comercial que retengan esos registros, mediante una orden judicial o a pedido de una autoridad pública.

1.4 ¿Monitoreo del espectro o vigilancia masiva?

COLOMBIA: La Ley 1.621, que regula las actividades de inteligencia, contiene una definición muy general de la vigilancia de las comunicaciones, lo que deja un amplio margen para potenciales abusos:

> *Las actividades de inteligencia y contrainteligencia comprenden actividades de monitoreo del espectro electromagnético debidamente incorporadas dentro de órdenes de operaciones o misiones de trabajo. La información recolectada en el marco del monitoreo del espectro electromagnético en ejercicio de las actividades de inteligencia y contrainteligencia, que no sirva para el cumplimiento de los fines establecidos en la presente Ley, deberá ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia. El monitoreo no constituye interceptación de comunicaciones.*
>
> *La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberá someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales.*

La Corte Constitucional de Colombia interpretó este lenguaje general como una autorización para permitir a las agencias el monitoreo de todo el espectro electromagnético,[50] sin autorización judicial independientemente de los medios tecnológicos que se empleen.

50 Comisión Europea, Comité Científico, Terminología Técnica – Glosario. http://ec.europa.eu/health/opinions/es/lamparas-bajo-consumo/glosario/def/espectro-electromagnetico.htm

Asimismo, esta disposición no autoriza de manera explícita la vigilancia masiva: según la jurisprudencia que aprobó la nueva Ley de Inteligencia, la Corte Constitucional hace hincapié en que la interceptación sólo está permitida durante las investigaciones penales y debe mediar una autorización judicial. En virtud de esta ley, las agencias de inteligencia tienen permitido monitorear el espectro, que en teoría difiere de la interceptación de las comunicaciones, según la Corte. Esta ley no brinda una definición de "monitoreo del espectro". Sin embargo, ya que la Ley 1.621 establece claramente que "el monitoreo no constituye interceptación de comunicaciones" —una frase que puede tener varias interpretaciones— es posible que la ley sea usada con ese mismo propósito.

De hecho, puede que esto ya haya ocurrido: durante los últimos años, sin ninguna autorización legal manifiesta, se han desarrollado varios programas de vigilancia masiva. Se supone que estos programas deben desplegarse mediante mecanismos como la Plataforma Única de Monitoreo y Análisis (PUMA) y el Sistema Integral de Grabación Digital (SIGD).

Contexto

Durante un breve periodo a comienzos de los años 2000, los colombianos fueron objeto de vigilancia mediante una plataforma llamada Esperanza, diseñada para espiar comunicaciones telefónicas determinadas. En 2009, los colombianos se asombraron al enterarse de esta vigilancia, y de cómo las agencias de inteligencia (DIPOL y DAS) habían interceptado las comunicaciones telefónicas de periodistas, partidos políticos de la oposición, defensores de los derechos humanos, e incluso las de jueces que habían trabajado durante el mandato de Álvaro Uribe.[51] Este escándalo causó la reestructuración de las agencias de inteligencia, junto con el desmantelamiento del DAS. Los miembros del DAS fueron procesados por el crimen de interceptación ilegal.[52]

Además de la plataforma Esperanza, existe un programa de interceptación llamado PUMA, adquirido en 2007 y administrado por la Dirección de Investigación Criminal e Interpol (DIJIN)—la rama criminalística de la policía.[53] Con el objetivo de recopilar y registrar información personal de interés para las investigaciones penales, esta plataforma está conectada directamente a la red central de Internet y al tráfico telefónico.[54]

51 Privacy International, "Un estado en la sombra: vigilancia y orden público en Colombia", (2015). https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

52 Privacy International, "Un estado en la sombra: vigilancia y orden público en Colombia," agosto 2015. https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

53 Privacy International. "Shadow State: Un estado en la sombra: vigilancia y orden público en Colombia" (2015). https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

54 Juan Camilo Rivera y Katitza Rodriguez, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Colombia", *Comisión Colombiana de Juristas, Electronic Frontier Foundation, & Fundación Karisma,* (2016). https://necessaryandproportionate.org/country-reports/colombia

La DIPOL (categorizada como agencia de inteligencia) usa su propio programa de vigilancia desde 2005: *El Sistema Integrado de Grabación Digital de la Dirección de Inteligencia Policial* es un programa que combina datos biométricos, registros públicos de redes sociales y otros datos disponibles para la creación de perfiles.[55]

Según el artículo 43 de la Ley de Inteligencia, las agencias de inteligencia son capaces de acceder a los registros pertenecientes a la policía judicial por razones de seguridad nacional. Aun así, dichas acciones deben llevarse a cabo de conformidad con el marco legal sobre derechos humanos de Colombia. Esto quiere decir que estas agencias realmente pueden obtener acceso a los datos interceptados por PUMA y Esperanza, debido a que actualmente los administra la policía judicial colombiana.[56]

La Fiscalía ha puesto en tela de juicio la legalidad de estas herramientas. Cree que incrementar las capacidades de interceptación de PUMA (al agregar hasta 20.000 líneas telefónicas más) "puede violar derechos de intimidad".[57] En la misma entrevista, el Procurador General Eduardo Montealegre dijo al diario colombiano, El Tiempo:

> *Puede conllevar al uso indiscriminado de la interceptación como herramienta de investigación en casos en los que esa invasión de derechos fundamentales ni siquiera es necesaria en la lucha contra la criminalidad [...]. Ningún otro organismo del Estado [diferente de la Fiscalía] está facultado para ordenar la interceptación de comunicaciones o administrar los equipos que sirven para esto. Es una garantía con la que cuentan todas las personas frente a su derecho legítimo a la intimidad y a la privacidad", señaló Montealegre.*

El año pasado, un e-mail particular de las filtraciones del Hacking Team sugería que la Agencia Antidroga estadounidense estaba llevando a cabo tareas de vigilancia masiva en Colombia al instalar equipos en la embajada estadounidense en Colombia "que recibiría todo el tráfico de los proveedores de servicio de Internet colombianos".[58]

---

55 Privacy International. "Shadow State: Un estado en la sombra: vigilancia y orden público en Colombia" (2015). https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

56 Colombia, Ley 1.621 de 2013, art. 43, http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201.621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

57 "Fiscalía le dice 'no' a sistema de interceptación 'Puma' de la Policía", *El Tiempo,* (2014), http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092.

58 Ryan Gallagher, "Mails de Hacking Team exponen propuestas de un escuadrón de la muerte, negociaciones secretas con el Reino Unido y mucho más", [Emails Expose Proposed Death Squad Deal, Secret UK Sales Push and Much More], *The Intercept*, (2015). https://theintercept.com/2015/07/08/hacking-team-emails-exposed-death-squad-uk-spying/ *Vea también el e-mail filtrado de Hacking Team.*

1.5 Las leyes de inteligencia imprecisas son propensas al abuso

ARGENTINA: El marco regulatorio para las actividades de inteligencia incluye la Ley 25.520 sobre Inteligencia Nacional,[59] aprobada en 2001, y la Ley 27.126, aprobada recientemente: ambas leyes modificaron sustancialmente la legislación anterior.[60] Estas leyes exigen al sistema de inteligencia argentino funcionar en estricta conformidad con las disposiciones de la Constitución Nacional y las normas legales y reglamentarias vigentes. Sin embargo, este marco regulatorio da lugar a actividades estatales discrecionales. Por ejemplo, la ley de inteligencia nacional establece que es la "autoridad máxima" de cada agencia del sistema de inteligencia quien ordenará las actividades de vigilancia.[61] No obstante, la ley también indica que en "casos de urgencia", estas actividades podrán ser iniciadas por otros, con la condición de ser informadas de manera inmediata a las autoridades máximas. Al no brindar una definición completa de "caso de urgencia", se da lugar a que ocurran vulneraciones en los derechos fundamentales. Ante la falta de una supervisión pública adecuada de las actividades de inteligencia, esta situación solo empeorará.

Sobre la base del Principio de Legalidad, el decreto emitido por la legislatura argentina llamado Nueva Doctrina de Inteligencia Nacional es cuestionable. Tiene como propósito instalar los nuevos objetivos y actividades de la recientemente creada Agencia Federal de Inteligencia en el contexto de la reestructuración de los servicios de inteligencia en el país. Como mencionamos anteriormente, esta nueva doctrina se origina mediante un decreto emitido por el poder ejecutivo y, como tal, no se discutió en el Congreso ni se debatió de manera pública. Esta doctrina amplía las definiciones de "atentados contra el orden constitucional", lo cual puede traer problemas en cuanto a la legalidad, ya que las definiciones son poco precisas.[62] Cabe señalar que el marco jurídico anterior ha sido modificado por varios reglamentos emitidos por la nueva administración, que formó gobierno en diciembre del 2015. Aún cuando la nueva administración se sitúa, ideologicamente, en el extremo opuesto del gobierno anterior, la nueva doctrina de inteligencia nacional no ha sido revocada, expresamente, ni la ha reemplazado con un documento que indique propósitos similares. Sin embargo, la nueva administración eliminó los mecanismos de supervisión, que el gobierno anterior había creado hacia el final de su mandato.[63]

---

https://www.documentcloud.org/documents/2160947-dea-amp-hacking-team-surveillance-in-colombia.html

59 Argentina, Ley No. 25.520 sobre Inteligencia Nacional, Boletín Oficial del 6 de diciembre de 2001.

60 Argentina, Ley No. 27.126 sobre la creación de la Agencia Federal de Inteligencia, Boletín Oficial del 5 de marzo de 2015.

61 Argentina, Ley No. 25.520 sobre Inteligencia Nacional, Boletín Oficial del 6 de diciembre de 2001, art. 5.

62 Argentina, Decreto No. 1.311/15, Boletín Oficial del 6 de julio de 2015, Anexo 1.

COLOMBIA: La Ley 1.621 de 2013 regula las actividades de inteligencia y contrainteligencia. Esta ley no define de manera precisa los propósitos por los cuales son legales las actividades de inteligencia (como veremos más abajo con respecto al objetivo legítimo). Adicionalmente, esta ley le brinda al poder ejecutivo la capacidad de emitir decretos que establezcan los parámetros para la desclasificación de la información.[64] Por otro lado, puede que los jueces no tengan acceso a la información clasificada cuando esta represente una amenaza para la seguridad nacional (esto queda a criterio de las agencias de inteligencia).[65] La Corte Constitucional de Colombia apoyó esta delegación de poder, argumentando que para todos los casos la ley brinda criterios claros sobre los cuales se pueden basar las regulaciones.[66] Así, habiéndole delegado el poder de alterar los niveles de clasificación, el poder ejecutivo está facultado para definir los criterios para la clasificación de la información. Las agencias de inteligencia y contrainteligencia están a cargo de aplicar dichos criterios en casos concretos.[67] Sin embargo, los momentos en que la confidencialidad de la información represente una limitación al derecho de acceso a la información deberían estar aclarados en una ley formal, de conformidad con el Principio de Legalidad, sin dejarlos a criterio del poder ejecutivo.[68]

BRASIL: La Ley 9.883 de 1999 creó el Sistema Brasileño de Inteligencia (SISBIN), que comprende diferentes agencias estatales, incluyendo el organismo principal, la Agencia Brasileña de Inteligencia (ABIN). La ABIN[69] tiene a cargo la planificación, ejecución, monitoreo y control de las actividades de inteligencia. Por esto, tiene acceso a la información recopilada por otras autoridades brasileñas mediante el SISBIN.

No queda claro cómo ocurre el intercambio de información entre el SISBIN y la ABIN, de acuerdo al informe de EFF e InternetLab.[70] La ley menciona específicamente el intercambio, y no existen mecanismos de transparencia vigentes que permitan al ámbito público monitorear el proceso. Por ejemplo, la ABIN no posee la facultad de interceptar comunicaciones, porque ni la Constitución de Brasil ni la legislación sobre interceptaciones

63 *Ver* ADC. "Ciberseguridad en la era de la vigilancia masiva." (2016). https://adcdigital.org.ar/wp-content/uploads/2016/06/ciberseguridad-argentina-ADC.pdf

64 Colombia, Ley 1.621 de 2013, art. 37.

65 Colombia, Ley 1.621 de 2013, art. 34.

66 Colombia, Corte Constitucional, sentencia C-540 de 2012.

67 El gobierno de Colombia dispuso regulaciones sobre los niveles de clasificación de la información de inteligencia y contrainteligencia mediante el decreto 857 de 2014.

68 Colombia, Ley 172 de 2014.

69 Extracto reporte de Brasil, Dennys Antonialli, Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Brasil", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

70 Extracto reporte de Brasil, Dennys Antonialli, Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Brasil", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

le brinda ese poder. Sin embargo, la ABIN puede ser capaz de conseguir datos obtenidos por la interceptación de las comunicaciones mediante un mecanismo de cooperación con otras entidades estatales.[71] En 2008, *Folha de São Paulo* reveló que la ABIN tiene acceso indirecto a las comunicaciones interceptadas desde el Sistema Policial (*Guardião*).[72] Además, si la Secretaría de Ingresos Federales de Brasil conserva los documentos de facturación de las compañías telefónicas en su base de datos, la ABIN tendría acceso a los registros telefónicos de los usuarios.

MÉXICO: La Ley de Seguridad Nacional autoriza al Centro de Investigación y Seguridad Nacional (CISEN) a interceptar comunicaciones privadas cuando exista una "amenaza inminente a la seguridad nacional".[73] El artículo 5 de esta ley define de manera muy general las "amenazas a la seguridad nacional", lo cual puede usarse para fijar como blanco a las ONG internacionales que forman parte del activismo en defensa de la privacidad. El artículo dispone lo siguiente:

1. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;

2. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;

3. Actos que impidan a las autoridades actuar contra la delincuencia organizada;

4. 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;

5. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;

6. Actos en contra de la seguridad de la aviación;

7. Actos que atenten en contra del personal diplomático;

8. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;

9. Actos ilícitos en contra de la navegación marítima;

---

71 Brasil, Juez Adilson Vieria Macabul, Suprema Corte de Justicia, habeas corpus 149250-SP, (2012). http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

72 Folha de São Paulo, "El acceso de la Abin a El Guardián causa controversia", (2008). http://www1.folha.uol.com.br/fsp/brasil/fc1211200805.htm

73 México, Ley de Seguridad Nacional. Artículos 33 - 49.

10. Todo acto de financiamiento de acciones y organizaciones terroristas;

11. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia; y,

12. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.[74]

1.6 Falta de precisión sobre las autoridades legales que pueden usar software malicioso, simuladores de torres de telefonía, u otras nuevas tecnologías de espionaje

Las nuevas tecnologías han planteado preguntas legales sobre las circunstancias bajo las cuales los latinoamericanos pueden esperar que sus datos estén a salvo del acceso de la vigilancia gubernamental. En su momento, la "vigilancia de las comunicaciones" consistía casi de manera exclusiva en las escuchas telefónicas; la escucha y/o la grabación de comunicaciones telefónicas.

Es por esto por lo que muchas leyes que regulan la vigilancia electrónica se siguen enfocando en las escuchas telefónicas. Rara vez hacen referencia a los recientes avances tecnológicos en el área de las comunicaciones electrónicas — como Internet — o a las técnicas de vigilancia.

Una de las técnicas más comunes que difiere significativamente de las escuchas telefónicas es el uso de software malicioso que infecta las computadoras de las personas para obtener acceso a las comunicaciones almacenadas en ellas o a las que pasaron por ellas. Otra es el uso de los recolectores IMSI, dispositivos que imitan a las torres de telefonía celular y son capaces de detectar la presencia de aparatos móviles e interceptar llamadas realizadas en un área geográfica.

Igual que las escuchas, estas tecnologías son invasivas y subrepticias, pero también plantean distintas preocupaciones sobre la privacidad y cuestiones legales que son muy diferentes a las de las tradicionales escuchas.

Estos, junto con otros desarrollos, hacen que la frase "vigilancia de las comunicaciones" comprenda un rango de técnicas y actividades mucho más amplias hoy en día en comparación con el pasado, momento en el que se redactaron las leyes sobre escuchas. Esta frase puede incluir una gama de distintos medios tecnológicos nuevos y de fuentes de datos que se usen para interferir en la privacidad de las comunicaciones, como el rastreo de la ubicación, registro de direcciones IP, software malicioso y de hackeo del gobierno, y actos que atentan contra los teléfonos móviles. La legislación antigua a menudo mantiene diferentes categorías de información protegida (o desprotegida), aun cuando las nuevas

74 México, Ley de Seguridad Nacional, art. 5.

fuentes de información y técnicas de análisis pueden fácilmente usarse para sacar conclusiones sensibles sobre los individuos y grupos de personas.

Al reconocer el amplio alcance del panorama actual de vigilancia, un grupo internacional de expertos, del cual formamos parte, propone que la definición de vigilancia de las comunicaciones incluya "monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas".[75]

Sin embargo, las leyes que se usan para autorizar estas novedosas tecnologías de vigilancia en América Latina ya quedaron desactualizadas o incompletas, y casi todos los órganos legislativos de la región no han considerado cuidadosamente cuándo o bajo qué circunstancias se deben usar esas tecnologías, si es que dicho uso resulta necesario. Por lo tanto, puede que se adopten las nuevas tecnologías de espionaje mediante un control legal mínimo, basado en interpretaciones explícitas o implícitas, que exime los controles de privacidad o que indica que los datos que obtienen no se encuentran completamente protegidos.

Hemos encontrado que, bajo esa legislación, muchos estados latinoamericanos adquieren nuevas tecnologías de espionaje, incluyendo la compra de software malicioso. *The Citizen Lab* y el Centro Canadiense para Estudios de Seguridad Global (*Canada Centre for Global Security Studies Munk School of Global Affairs*) revelaron la existencia de servidores de comando y control FinSpy, FinFisher, un intrusivo software de vigilancia remota desarrollado por Gamma International, en varios países, incluyendo a México[76] y Panamá en 2013,[77] y a Venezuela y Paraguay en 2015.[78] Este software espía desarrollado por la firma

75 Necessary and Proportionate Coalition, *Necesarios & Proporcionados*, (2014). http://necessaryandproportionate.org/principles; Necessary and Proportionate Coalition, *Necessary & Proportionate Global Legal Analysis*, (2014). http://necessaryandproportionate.org/global-legal-analysis

76 Bill Marzcak, Claudio Guarnieri, John Scott-Railton, y Morgan Marquis-Boire, "Solo haces doble clic: La proliferación global de FinFisher", [You Only Click Twice: FinFisher's Global Proliferation], *Citizen Lab y el Canada Centre for Global Security Studies Munk School of Global Affairs, Universidad de Toronto,* (2013). https://citizenlab.org/wp-content/uploads/2009/10/You-Only-Click-Twice-FinFisher's-Global-Proliferation.pdf

77 Morgan Marquis-Boire et al., "Únicamente para que ellos lo vean: La comercialización del espionaje digital" [For Their Eyes Only: The Commercialization of Digital Spying], *Citizen Lab y el Canada Centre for Global Security Studies Munk School of Global Affairs, Universidad de Toronto*, (2013). https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf

78 Adam Senft, Bill Marczak, Irene Poetranto, John Scott-Railton, y Sarah McKune, "No le preste atención al servidor detrás del proxy: Un mapeo de la continua proliferación de FinFisher" [Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation], *Citizen Lab y el Canada Centre for Global Security Studies Munk School of Global Affairs, Universidad de Toronto*, (2015). https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

alemana Gamma International es comercializado y vendido a autoridades de aplicación de la ley y agencias de inteligencia por el grupo inglés Gamma Group.[79]

Dos filtraciones importantes revelaron también nuevas perspectivas sobre el amplio mercado de las tecnologías de vigilancia. La primera, relacionada con FinFisher/FinSpy, salió a la luz en agosto de 2014.[80] Se publicaron 40 gigabytes de datos internos, incluyendo notas de lanzamiento, listas de precios, y código fuente. La segunda filtración, relativa a la tristemente conocida compañía italiana Hacking Team, la cual vende software espía, fue publicada en julio de 2015. Los atacantes vulneraron los servidores de la compañía y dieron a conocer 400 gigabytes de datos internos y comunicaciones que la empresa había mantenido con clientes. Esos documentos revelaron que Brasil, Colombia, Chile, Ecuador, Honduras, México, y Panamá habían comprado licencias para el sistema de control remoto de Hacking Team.[81]

Las filtraciones también dieron a conocer que Argentina, Guatemala, Paraguay, Perú, Uruguay, y Venezuela habían comenzado a negociar con Hacking Team. Sin embargo, estas filtraciones no dejaron conocer si realmente alguno de esos países había efectuado alguna compra.[82]

El uso de estas tecnologías subrepticias e intrusivas no debería tener lugar sin una autorización legal específica, y debería permitirse solamente si no hay otras maneras disponibles que sean menos invasivas para obtener la información. En una declaración, la Relatoría Especial para la Libertad de Expresión de la Organización de los Estados Americanos expresó:

> *[D]e acuerdo con los estándares internacionales, el uso de programas o sistemas de*

79 Bill Marzcak, Claudio Guarnieri, John Scott-Railton, y Morgan Marquis-Boire, "Solo haces doble clic: La proliferación global de FinFisher", [You Only Click Twice: FinFisher's Global Proliferation], *Citizen Lab y el Canada Centre for Global Security Studies Munk School of Global Affairs, Universidad de Toronto,* (2013). https://citizenlab.org/wp-content/uploads/2009/10/You-Only-Click-Twice-FinFisher's-Global-Proliferation.pdf

80 Joseph Cox, "Hacker afirma haber filtrado 40GB de documentos gubernamentales sobre la herramienta de espionaje FinFisher" [A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher], (2014). http://motherboard.vice.com/read/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher

81 Gisela Pérez de Acha, "Hacking Team malware para la vigilancia en América Latina," *Derechos Digitales*, (2016). https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf. *Vea también* Juan Diego Castañeda, "Cuando el Estado 'hackea', un análisis de la legitimidad del uso de las herramientas de hacking en Colombia", *Fundación Karisma*, (2015). https://karisma.org.co/wp-content/uploads/2015/12/When-the-State-hackea-D.pdf

82 Gisela Pérez de Acha, "Hacking Team malware para la vigilancia en América Latina," *Derechos Digitales*, (2016). https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf. *Vea también* Juan Diego Castañeda, "Cuando el Estado 'hackea', un análisis de la legitimidad del uso de las herramientas de hacking en Colombia", *Fundación Karisma*, (2015). https://karisma.org.co/wp-content/uploads/2015/12/When-the-State-hackea-D.pdf

vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación. Tales restricciones deben ser estrictamente proporcionadas y cumplir con las normas internacionales sobre el derecho a la libertad de expresión. Esta oficina ha expresado que la vigilancia de las comunicaciones y las injerencias a la privacidad que excedan lo estipulado en la ley, que se orienten a finalidades distintas a las autorizadas por ésta o las que se realicen de manera clandestina deben ser drásticamente sancionadas. Esta injerencia ilegítima incluye aquellas realizada por motivos políticos contra defensores de derechos humanos, periodistas y medios de comunicación independientes.[83]

Al comparar las legislaciones internas de los países analizados, descubrimos lo siguiente:

1. En Chile, Paraguay, Guatemala, Honduras, y Uruguay, los vacíos legales son tan amplios que es posible interpretar una autorización del uso de cualquier tipo de tecnología de vigilancia actual o futura, como el software malicioso o los recolectores IMSI, o cualquier tipo de tecnología que pueda desarrollarse en el futuro;

2. Si bien muchos de los Estados que analizamos en este reporte han adquirido software malicioso, no existen en ninguno de los 13 países incluidos disposiciones legales específicas que faculten a las autoridades gubernamentales para usar ese malware o recolectores IMSI;

3. En al menos uno de los países estudiados, autoridades gubernamentales y compañías estatales adquirieron de manera ilegal herramientas de vigilancia, incluyendo software malicioso, a pesar de no haber tenido autorización legal o constitucional para llevar a cabo actividades de vigilancia; y

4. México ha usado software malicioso en contra de partidos políticos de la oposición y periodistas.

Los ejemplos que siguen ponen de relieve prácticas preocupantes en la región.

MÉXICO: México no cuenta con ninguna ley que específicamente autorice el uso de malware. Filtraciones recientes revelaron que México es el principal cliente de Hacking Team.[84] Peor aún, salió a la luz que los gobernadores de los estados de Querétaro, Puebla,

83 Relator Especial para la Libertad de Expresión, "La Relatoría Especial expresa preocupación ante la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio", (2005). http://www.oas.org/en/iachr/expression/showarticle.asp?artID=998&lID=1

84 Arturo Angel, "México, el principal cliente de una empresa que vende software para espiar". *Animal Político,* (2015). http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-

Campeche, Tamaulipas, Yucatán, Durango, y Jalisco compraron y acumularon malware poderoso, diseñado para atacar computadoras personales y teléfonos, a pesar de no contar con la autorización legal para llevar a cabo cualquier tipo de vigilancia. De la misma manera, la compañía estatal petrolera PEMEX (Petróleos Mexicanos) también fue indentificada como uno de los clientes de Hacking Team.[85] Las autoridades que tienen el poder para interceptar comunicaciones privadas en México son la Procuraduría General de la Nación junto con las fiscalías de las 31 organizaciones federativas y el Distrito Federal, la Comisión Nacional de Seguridad (Policía Federal), y el Centro de Investigación y Seguridad Nacional (Poder Ejecutivo).[86]

Para empeorar aún más las cosas, el gobierno de Puebla usó el software malicioso de Hacking Team para espiar de manera ilegal a oponentes políticos —incluyendo al Partido Acción Nacional (PAN)— en 2014. Además, el gobernador de Puebla realizó actividades de vigilancia en 2013 durante las elecciones estatales, momento en que se nombraban los puestos de alcaldía y del Congreso. También espiaba a académicos, periodistas, y oponentes políticos durante las últimas elecciones federales de Puebla.[87]

COLOMBIA: En este país no existe ley que autorice expresamente el uso de malware.[88] Sin embargo, las filtraciones sobre Hacking Team revelaron que la Policía Nacional de Colombia adquirió el software Galileo de Hacking Team para usarlo entre 2013 y 2016.[89] Anteriormente, la policía había negado estar asociada con Hacking Team, pero las filtraciones indicaron que la policía había, en efecto, comprado malware mediante el

---

cliente/

85 Daniel Hernández y Gabriela Gorbea, "México es el mejor cliente de Hacking Team —sin dudas" [Mexico Is Hacking Team's Biggest Paying Client — By Far], VICE, https://news.vice.com/article/mexico-is-hacking-teams-biggest-paying-client-by-far, Sebastián Barragán, "Equipo de espionaje en México: sin control legal suficiente ni transparencia", Aristegui Noticias, (2016). http://aristeguinoticias.com/1804/mexico/equipo-de-espionaje-en-mexico-sin-control-legal-suficiente-ni-transparencia/, PEMEX, "Gobiernos e inteligencia mexicanos, expuestos como clientes de compañía de espionaje" [Mexican intelligence and governments, outed as clients of spy company], El Universal, http://www.eluniversal.com.mx/articulo/english/2015/07/6/pemex-mexican-intelligence-and-governments-outed-clients-spy-company

86 Luis Fernando García, "México: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México" *Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales* (2016). https://necessaryandproportionate.org/country-reports/mexico

87 Ernesto Aroche, "El gobierno de Puebla usó el software de Hacking Team para espionaje político," Animal Político, (2015). http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/

88 Carolina Botero y Pilar Sáenz, "En Colombia, el PUMA no es como lo pintan", *Digital Rights Latin America & The Caribbean*, (2015). http://www.digitalrightslac.net/en/en-colombia-el-puma-no-es-como-lo-pintan/

89 Privacy International, "Un estado en la sombra: vigilancia y orden público en Colombia", (2015). https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

intermediario Robotec.[90] A raíz de tales filtraciones, la policía colombiana expresó que no había tenido relación alguna con Hacking Team, sino con Robotec, y que "el propósito de esta compra fue potencializar la capacidad de detección de amenazas del terrorismo y la criminalidad organizada en el ciberespacio colombiano".[91]

En 2015, Vicky Davila, periodista que informa sobre corrupción policial, develó un escándalo sexual que estaba profundamente enraizado en el sistema policial colombiano e involucraba a varios oficiales de policía de alto rango.[92] Después de que explotó el escándalo, Davila afirmó que sus dispositivos de trabajo, y los de sus compañeros, fueron infectados por software malicioso.[93]

ARGENTINA: Argentina no cuenta con ninguna ley que de manera expresa autorice el uso de malware.[94] La legislación de este país prevé solo la interceptación de comunicaciones cuando medie una orden emitida por un juez, y por un periodo de tiempo que no exceda los 30 días. El Código Procesal Penal establece que las comunicaciones pueden ser interceptadas para investigar un crimen, pero sólo de conformidad con los principios de necesidad, proporcionalidad, razonabilidad, e idoneidad.[95]

Sobre la base de información de acceso público, no hay evidencia para asegurar que Argentina haya comprado productos de Hacking Team. No obstante, las filtraciones

---

90 Para una investigación más pormenorizada, lea a Juan Diego Castañeda, "Cuando el Estado 'hackea', un análisis de la legitimidad del uso de las herramientas de hacking en Colombia", Fundación Karisma, 2015. https://karisma.org.co/wp-content/uploads/2015/12/When-the-State-hackea-D.pdf

91 Semana, Cuando hackean a los hackers, http://www.semana.com/nacion/articulo/los-lios-de-hacking-team-por-informacion-hackeada/434391-3, Diana Carolina Durán Núñez, El software espía de la Policía, El Espectador, Julio de 2015, http://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980

92 El Tiempo, "Las investigaciones pendientes en el escándalo de la Policía," (2016). *Vea también* Juan Camilo Rivera y Katitza Rodriguez, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Colombia," *Comisión Colombiana de Juristas, Electronic Frontier Foundation, & Fundación Karisma,* (2016). https://necessaryandproportionate.org/country-reports/colombia

93 Fundación Karisma, "El tal 'hackeo' sí existe," (2015). https://karisma.org.co/el-tal-hackeo-si-existe/

94 Para una investigación más pormenorizada, lea a Daniela Schnidrig y Verónica Ferrari, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina," *Centro de Estudios en Libertad de Expresión y Acceso a la Información, y Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/argentina

95 Daniela Schnidrig y Verónica Ferrari, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina," *Centro de Estudios en Libertad de Expresión y Acceso a la Información, y Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/argentina

revelaron que el gobierno argentino se comunicó con Hacking Team en varias ocasiones, y la compañía italiana presentó sus productos al Ministerio de Seguridad de la Nación, a la Dirección Nacional de Inteligencia Criminal, al Procurador General, y a la Unidad de Investigaciones Complejas, entre otros.[96] Por el momento, el gobierno argentino no ha emitido una declaración oficial que admita o niegue tales reuniones.

Existen algunos acontecimientos anecdóticos que indican que en Argentina se ha usado software malicioso. El abogado Alberto Nisman ejerció como fiscal federal y era conocido en el país por investigar el atentado más letal sufrido por Argentina: el ataque a la AMIA (Asociación Mutual Israelita Argentina) en Buenos Aires en 1994, que, hasta el día de hoy, sigue sin esclarecer. En 2015, Nisman fue hallado muerto en su hogar, y, según un análisis técnico, el teléfono del fiscal mostraba rastros de malware.

Sin embargo, debido a que el malware estaba dirigido originalmente hacia la computadora de Nisman, el teléfono no fue infectado.[97] El experto que llevó a cabo el análisis del malware en el teléfono de Nisman llegó a la conclusión de que quienquiera que haya estado detrás del ataque de malware era la misma persona que estaba vigilando a Jorge Lanata, periodista independiente argentino, ya que encontró características en común entre los tipos de software utilizados en ambos casos. Aunque existen claros indicios de que fue una persona del gobierno la que estaba detrás de estos ataques, no se han atribuido a un gobierno en particular hasta ahora.[98]

HONDURAS: Honduras posee una ley especial que regula la interceptación de las comunicaciones privadas.[99] Con arreglo a esta ley, la interceptación de las comunicaciones

96 Hacking Team, Reuniones en Argentina, https://wikileaks.org/hackingteam/emails/emailid/587154, y reporte sobre Argentina, https://wikileaks.org/hackingteam/emails/emailid/765194, y reporte sobre Argentina, con el orden del día definitivo adjunto, https://wikileaks.org/hackingteam/emails/emailid/596983 *Vea también,* Asociación por los Derechos Civiles, *La ADC alerta: software de interceptación y vulneración a los derechos humanos*, (2015). https://adcdigital.org.ar/wp-content/uploads/2015/08/Software-de-interceptacion-y-DDHH.-Informe-ADC.pdf

97 Daniela Schnidrig y Verónica Ferrari, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina," *Centro de Estudios en Libertad de Expresión y Acceso a la Información, y Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/argentina

98 Morgan Marquis-Boire, "Dentro de la campaña de software espía en contra de los argentinos problemáticos", [Inside The Spyware Campaign Against Argentine Troublemakers] *The Intercept,* (2015). https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/ *Vea también* Daniela Schnidrig y Verónica Ferrari, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina", *Centro de Estudios en Libertad de Expresión y Acceso a la Información, y Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/argentina

99 Para un análisis pormenorizado de las leyes de vigilancia en Honduras, lea a Fundación Acceso "¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados

puede ser llevada a cabo mediante "técnicas especiales de investigación". Esta definición está redactada de una forma tan general que se podría interpretar que autoriza el uso de malware y quizás de cualquier otra tecnología de vigilancia:

> *[E]s una técnica especial de investigación, que consta en el procedimiento a través del cual se escucha, capta, registra, guarda, graba, u observa, por parte de la autoridad, sin el conocimiento de sus titulares o participantes, una comunicación que se efectúa, mediante cualquier tipo de transmisión, emisión o recepción de signos, símbolos, señales escritas, imágenes, sonidos, correos electrónicos o información de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros medios, sistemas electromagnéticos, telefonía [...] medios informáticos o telemáticos, o de naturaleza similar o análogo, así como la comunicación que se efectúe a través de cualquier medio o tipo de transmisión.*[100]

Las únicas agencias gubernamentales autorizadas que pueden solicitar una orden a un juez para interceptar comunicaciones son el Ministerio Público, la Policía Nacional, y la Procuraduría General de la Nación (artículo 7). El único organismo autorizado para interceptar comunicaciones es la Unidad de Interceptación de Comunicaciones.

La Ley de Inteligencia Nacional autoriza a la Dirección Nacional de Investigación e Inteligencia (DNII) a realizar tareas de vigilancia con el propósito de proteger los derechos de los ciudadanos y la seguridad nacional.

En 2014, la agencia de inteligencia de Honduras, DNII, adquirió el software Galileo de Hacking Team.[101]

BRASIL: No existen regulaciones específicas sobre hackeo por parte del gobierno en Brasil. Sin embargo, el artículo 158 de la Ley 13.097 sí permite a las autoridades eludir la licitación pública. Esto significa que las autoridades no necesitan divulgar públicamente si adquirieron tecnología de vigilancia para uso en investigaciones policiales.[102]

En mayo de 2015 la Policía Federal de Brasil compró software RCS de Hacking Team

---

para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos", 2015. http://acceso.or.cr/files/investigacion-resumen-ejecutivo.pdf

100 Honduras, Ley de intervenciones de las comunicaciones, sección 3, no. 11. http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Especial%20sobre%20Intervencion%20de%20las%20Comunicaciones%20Privadas%20(8,2mb).pdf

101 Gisela Pérez de Acha, "Hacking Team malware para la vigilancia en América Latina," *Derechos Digitales,* (2016). https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf.

102 Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

mediante una compañía intermediaria, YasniTech.[103] La agencia brasileña pagó 75 mil reales al intermediario, y Yasnitech pagó a Hacking Team 25 mil euros por una prueba de tres meses de ese software.[104] Según las filtraciones de Hacking Team, un juez autorizó a la Policía Federal a usar "una aplicación para recopilar datos de teléfonos bajo investigación" por 15 días.[105] La Policía Federal de Brasil no admitió ni desmintió el acuerdo con Hacking Team.[106]

PARAGUAY: No existen regulaciones específicas sobre hackeo por parte del gobierno en Paraguay. Sin embargo, el artículo 200 del Código Procesal Penal contiene un gran vacío legal que puede interpretarse como una autorización para el uso de cualquier tipo de tecnología y técnica de vigilancia. Esta disposición establece que un juez puede ordenar la interceptación de las comunicaciones de cualquier persona acusada, "cualquiera sea el medio técnico utilizado para conocerlas".

Según una investigación realizada por el diario paraguayo ABC Color, la Secretaría Nacional Antidrogas (SENAD) adquirió la plataforma FinFisher en noviembre de 2012. ABC Color develó el recibo de compra, así como también un registro de la entrega del sistema.[107] En mayo de 2016, dos semanas después de la publicación del reporte "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Paraguay" de EFF y TEDIC,[108] el Ministro de la SENAD hizo referencia a los hallazgos del reporte y finalmente

---

103 Vea la lista de clientes de Hacking Team: https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/5%20-%20Analisi%20Fatturato/2015/Customer%20History.xlsx *Vea también* Re: Brasil - PoCs y Demos -- Feedback sobre la primera reunión con la Policía Civil - Departamento de Inteligencia SP [Re: Brazil - POCs and Demos -- Feedback first meeting with Civil Police - SP Department of intelligence]: https://www.wikileaks.org/hackingteam/emails/emailid/440130

104 Vea la facturación filtrada de Hacking Team: *https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/1%20-%20Commesse/5%20-%20Commesse%202015/Commessa013.2015%20Yasnitech.xls*

105 Felipe Ventura, Las menciones a Brasil en los correos electrónicos filtrados de Hacking Team, 10 de julio, 2015, http://m.gizmodo.uol.com.br/brasil-e-hacking-team/Vea también: Natalia Viana, Hacking Brasil, http://apublica.org/2015/07/hackeando-o-brasil/. Dennys Antonialli, Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

106 Redação Linha Defensiva, "La PF estaba por cerrar contrato de espionaje millonario", *Linha Defensiva,* (2015).http://www.linhadefensiva.org/2015/07/pf-estava-para-fechar-contrato-milionario-de-espionagem/

107 ABC Color, *Senad gastó casi G. 200 millones solo en "montaje y configuración*", (2013). http://www.abc.com.py/edicion-impresa/judiciales-y-policiales/senad-gasto-casi-g-200-millones-solo-en-montaje-y-configuracion-590062.html?fb_comment_id=419236824858112_2094744#f1c83727667f9fc

108 Jorge Rolón Luna y Maricarmen Sequera, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Paraguay", *Electronic Frontier Foundation & TEDIC*, (2016). https://necessaryandproportionate.org/country-reports/paraguay

confirmó que Paraguay sí había comprado el software malicioso en 2012. El Ministro afirma que el software se usa como un "sistema de seguridad de georeferenciamiento".[109]

GUATEMALA: La legislación de Guatemala también brinda un poder sorprendentemente amplio que puede interpretarse como una autorización para el uso de cualquier tipo de tecnología y técnica de vigilancia. El artículo 48 de la Ley contra la Delincuencia Organizada contempla que cualquier comunicación que sea oral, escrita, telefónica, radiotelefónica, o informática que utilice el espectro electromagnético, así como también "cualesquiera de otra naturaleza" que exista en el futuro podrá interceptarse, grabarse y reproducirse con autorización judicial.

Las filtraciones de Hacking Team revelaron que el gobierno de Guatemala mantenía conversaciones con Hacking Team, aunque no se develó ninguna evidencia de compra.

URUGUAY: El artículo 5 de la Ley 18.494 sobre el Control y Prevención de Lavados de Activos y del Financiamiento del Terrorismo autoriza el uso de cualquier medio tecnológico disponible para la investigación de cualquier ofensa para facilitar su esclarecimiento. Una amplia interpretación de esta regla autoriza básicamente el uso de varios tipos de técnicas y tecnologías de vigilancia, como el malware o los recolectores IMSI.

La ley no designa a una autoridad legal específica de manera expresa y clara—lo cual es necesario para cumplir con la normativa internacional de derechos humanos de la Organización de los Estados Americanos.[110]

109 TEDIC, "Más preguntas y dudas sobre software malicioso adquirido por SENAD", (2016). https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/

110 Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Uruguay: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay", *Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/uruguay

2.
Objetivo Legítimo

Este Principio establece que las leyes sólo deberían permitir la vigilancia de las comunicaciones por parte de autoridades estatales específicas para lograr un objetivo legítimo que corresponda a un interés legal preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

Nuestro análisis de los marcos legales para la realización de vigilancia en los países incluidos en este estudio deja claro que la vigilancia de las comunicaciones es aceptable como objetivo legítimo si se lleva a cabo con propósitos probatorios, las investigaciones de crímenes graves, o por seguridad nacional. Sin embargo, la vigilancia digital es una fuerte tentación para los investigadores y los oficiales de policía.

Para prevenir el abuso, la ley debe especificar las situaciones en las que la vigilancia cumple un verdadero objetivo legítimo. Este Principio debería aplicarse también cuando a un juez se le solicite autorizar una medida de vigilancia determinada.

El Objetivo Legítimo, como lo definen los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, se basa en un alto estándar establecido por la Corte Constitucional de Alemania en 2008:[111]

> *[E]n particular, la Corte Constitucional alemana pronunció que las medidas sumamente intrusivas como el registro de una computadora por parte de las agencias de aplicación de la ley no pueden estar justificadas meramente mediante un interés general definido de manera tan general. La Corte Constitucional alemana mantuvo que tal medida debe estar justificada en base a evidencia de que exista "una amenaza concreta para un interés relevante y protegido legalmente", como las amenazas a la "vida, la integridad física o la libertad de una persona" o a "bienes públicos, cuyo riesgo amenaza la sola existencia del estado, o de las condiciones necesarias y fundamentales para la existencia humana".*[112]

Las mejores prácticas en esta área comprenden la legislación sobre vigilancia que contengan listas exhaustivas de crímenes específicos (o alguna otra definición clara y objetiva) y otras

111 Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis, (2014). http://necessaryandproportionate.org/global-legal-analysis

112 Dictamen en la Sentencia de la Corte Constitucional. 27 de febrero de 2008 (1 BvR 370/07 y 1 BvR 595/07).

restricciones legales que garantizan que no se violará ningún derecho humano.

Aunque el Principio de Objetivo Legítimo exige que cualquier acto de vigilancia de las comunicaciones debe tener un objetivo legítimo, la sección que sigue sólo explora los objetivos gubernamentales que en efecto son "legítimos" y hasta qué punto incorporan este principio a las leyes que regulan la vigilancia de las comunicaciones en la región.

La mayoría de los países que fueron investigados contienen leyes que limitan las prácticas de vigilancia sólo a los crímenes graves, pero en muchos casos estas leyes no consiguen especificar debidamente cuáles son los crímenes que se encuentran dentro de esta categoría. Las definiciones de algunos términos, como "terrorismo" y "cibercrimen", que aparecen en muchas leyes de la región, son tan generales que la mayoría de las técnicas de vigilancia invasiva se puede aplicar más allá de sus objetivos legítimos.

Debido a la preocupación que esto causa, el Relator Especial sobre la Libertad de Expresión y Opinión puso de relieve la imprecisión y falta de descripción del término "seguridad nacional", cuyo uso es generalizado en las legislaciones que regulan la vigilancia de las comunicaciones:

> *60. El uso de un concepto impreciso de seguridad nacional para justificar limitaciones invasivas del goce de los derechos humanos plantea serias preocupaciones. Este concepto tiene una definición amplia y, por consiguiente, es vulnerable a la manipulación del Estado como medio de justificar medidas dirigidas a grupos vulnerables como defensores de los derechos humanos, periodistas o activistas. También permite justificar el secreto a menudo innecesario en torno a investigaciones o actividades de las fuerzas del orden, socavando los principios de la transparencia y la rendición de cuentas.*[113]

Cuando se trata de la legislación que regula la vigilancia con fines de inteligencia, observamos que varios Estados nacionales definen de manera específica los objetivos legítimos, una práctica que debería adoptarse más ampliamente. Todos los Estados deberían seguir el camino de aquellos que expresamente prohíben el uso de vigilancia de inteligencia en una manera que discrimina en base a la raza, color, sexo, idioma, religión, opiniones políticas o de otra índole, origen social o nacional, propiedad, nacimiento o cualquier otra condición.

113 Frank La Rue, *Relator Especial sobre la Libertad de Expresión y Opinión*, A/HRC/23/40, (2013, párr. 58). http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

2.1 Restricciones sobre el objetivo legítimo

Es una buena práctica que los Estados limiten la lista de ofensas sobre las que se puede autorizar la vigilancia. A continuación brindamos cuatro ejemplos:

NICARAGUA: Los artículos 213 y 214 del Código Procesal Penal limitan la interceptación de las comunicaciones a una lista detallada de crímenes graves. Esta lista incluye el terrorismo, secuestro, crímenes relacionados con el narcotráfico, el lavado de activos, y el tráfico de armas internacional.[114]

GUATEMALA: La Ley contra la Delincuencia Organizada limita la interceptación de las comunicaciones a los casos en los que la prevención y la investigación de un crimen son necesarias. Estos casos comprenden crímenes organizados específicos y ofensas que tienen un impacto social importante.[115]

PERÚ: En virtud de la legislación penal, las autoridades judiciales pueden autorizar que un fiscal tome control de las comunicaciones que se encuentren bajo investigación preliminar o jurisdiccional, y sólo para una lista de ofensas específica: El secuestro, contrabando, pornografía infantil, robo agravado, extorsión, narcotráfico, crímenes de lesa humanidad, violaciones a la seguridad nacional y traición a la patria, malversación, corrupción, terrorismo, ofensas fiscales y aduaneras, lavado de activos, y cibercrimen están incluidos en dicha lista.[116]

BRASIL: La Ley 9.296 de 1996 prevé la interceptación de las comunicaciones con el propósito de investigar un crimen o hallar información durante un procedimiento penal mediante orden judicial, *ex-officio,* o a pedido de un funcionario de aplicación de la ley o de la Fiscalía General.[117] La interceptación de las comunicaciones queda prohibida cuando existan pruebas razonables de la responsabilidad o conspiración para cometer un crimen, cuando las pruebas se puedan obtener por otros medios, o cuando la sanción al sospechoso, si es declarado culpable, sea solo la detención (*detenção)*, común en los casos de delitos menores.

114 Nicaragua, *Código Procesal Penal 406*, (2001), y La Gaceta 243 y 244, (2001). http://legislacion.asamblea.gob.ni/Normaweb.nsf/%28$All%29/5EB5F629016016CE062571A1004F7C62

115 Guatemala, Ministerio del Interior, *Ley contra la Delincuencia Organizada,* art. 48, (2006). http://leydeguatemala.com/ley-contra-la-delincuencia-organizada/interceptaciones/10468/

116 Perú, Ley 27.697*, Código Penal y Código Procesal Penal.*

117 Brasil, Ley 9.296, art. 3, (1996).

2.2 Algunas leyes latinoamericanas incorporan aspectos del Principio de Objetivo Legítimo pero no logran acatarlo completamente

En vez de restringir las medidas de vigilancia intrusivas sólo a crímenes determinados, algunos Estados manejan la autorización de la vigilancia de manera distinta según el tipo de ofensa bajo investigación.

ARGENTINA: El marco legal de Argentina permite la interceptación de las comunicaciones sólo si se prueba que sería útil para combatir un crimen. Sin embargo, no especifica la gravedad de dicho crimen:

> *[E]n principio, el régimen legal argentino que prevé interceptaciones a las comunicaciones cumple con este requisito, en tanto establece que las interceptaciones serán realizadas de forma excepcional, con el objetivo de comprobar delitos complejos o de asegurar la defensa nacional y la seguridad interior.*[118]

CHILE: El régimen legal de Chile impone menos restricciones a la vigilancia relativa al terrorismo y al narcotráfico que a la relacionada con delitos comunes.[119] Para empeorar las cosas, la ley no contiene una definición clara del término "terrorismo". Esto da lugar a que los jueces apliquen las normas establecidas en la Ley Antiterrorismo discrecionalmente. En cambio, se aplican más medidas de protección a la vigilancia realizada para la investigación de delitos comunes. De hecho, para la investigación de delitos comunes —aquellos que conllevan una pena menor a la privación de la libertad por un periodo de cinco años— no se pueden llevar a cabo tareas de vigilancia:

> *Una crítica usual a la [Ley Antiterrorismo] es la definición que entrega sobre actividad terrorista, dado lo vaga e imprecisa que resulta*[120] *[...]. A su vez, dada la especial peligrosidad de este tipo de ilícitos, esta ley hace más laxo el estándar exigido para interceptar comunicaciones telefónicas y otro tipo de comunicaciones. Esta ley resta los varios requisitos exigidos en el Código Procesal Penal, reduciéndolos a no*

118 Daniela Schnidrig y Verónica Ferrari, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina", *Centro de Estudios en Libertad de Expresión y Acceso a la Información, y Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/argentina

119 *Vea* la Ley 18.314, que determina conductas terroristas, la Ley 20.000, que sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas, y el artículo 222 del Código Procesal Penal.

120 Instituto Nacional de Derechos Humanos (INDH). "Informe sobre cuestiones a considerar en una reforma de la Ley Antiterrorista a la luz de la observación de casos realizada por el Instituto Nacional de Derechos Humanos". Aprobado por el Consejo del Instituto Nacional de Derechos Humanos el 22 de julio de 2014. págs. 4-7. http://bibliotecadigital.indh.cl/bitstream/handle/123456789/655/Informe%20Ley%20Antiterrorista.pdf?sequence=1

interceptar comunicaciones entre el acusado y su abogado.[121]

En efecto, la Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos señala que las consideraciones subjetivas, arbitrarias y/o políticas desempeñaron un papel importante en la selección de casos en los que se ha aplicado la legislación antiterrorista:

> *Las diversas justificaciones planteadas han sido subjetivas y carentes de rigor legal. Esto se corrobora al comparar los casos en que se han presentado cargos terroristas y aquellos en que no. Es imposible distinguir una línea divisoria clara y consistente entre casos donde se han presentado cargos como delitos penales comunes (tales como, incendio premeditado, homicidio frustrado y delitos con armas de fuego) de aquellos en que se ha invocado la ley antiterrorista, a fin de agravar la pena y entregar ventajas procesales adicionales al fiscal. El Relator Especial concluye con reticencia que consideraciones subjetivas, arbitrarias y/o políticas han jugado un papel en la selección de esos casos donde se ha invocado la ley antiterrorista.*[122]

COLOMBIA: Si bien no existe una lista específica de los crímenes a los que se limita la interceptación de las comunicaciones, el régimen procesal penal autoriza la interceptación de las comunicaciones sólo con el propósito de recopilar evidencia durante investigaciones penales. Con arreglo al artículo 222 del Código Procesal Penal, el juez deberá, a pedido del fiscal, autorizar la interceptación y grabación de las comunicaciones durante procedimientos penales en los casos en que una persona haya cometido o participado en la preparación de un crimen, o cuando el acusado se enfrente a una pena de al menos cinco años y un día de privación de la libertad.

En el contexto de inteligencia, la Ley 1.621 de 2013 enumera los fines a los que se deben limitar las actividades de inteligencia y contrainteligencia, pero no los define de una manera adecuada. Específicamente, el artículo 4 enuncia los siguientes objetivos legítimos:

a) Asegurar la consecución de los fines esenciales del Estado, la vigencia del régimen democrático, la integridad territorial, la soberanía, la seguridad y la defensa de la Nación;

b) Proteger las instituciones democráticas de la República, así como los derechos de las

121 Valentina Hernández y Juan Carlos Lara, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile", *Derechos Digitales y Electronic Frontier Foundation* (2016). https://necessaryandproportionate.org/country-reports/chile

122 Naciones Unidas, Derechos Humanos, Declaración del Relator Especial de las Naciones Unidas sobre la promoción y la protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo, (2013). http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=13598, cita de Valentina Hernández y Juan Carlos Lara, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile," *Derechos Digitales y Electronic Frontier Foundation* (2016). https://necessaryandproportionate.org/country-reports/chile

personas residentes en Colombia y de los ciudadanos colombianos en todo tiempo y lugar –en particular los derechos a la vida y la integridad personal– frente a amenazas tales como el terrorismo el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas, municiones, explosivos y otros materiales relacionados, el lavado de activos, y otras amenazas similares; y

c) Proteger los recursos naturales y los intereses económicos de la Nación.

La ley no describe de manera específica estos objetivos, y no brinda ejemplos que provean un contexto o panorama en los que se debería recurrir a los servicios de inteligencia y contrainteligencia. Esta carencia de especificidad podría permitir a las agencias de inteligencia determinar por sí mismas los eventos que justifiquen actividades de inteligencia y contrainteligencia, lo cual deja toda actividad de vigilancia sujeta a la consideración de las agencias.

2.3 El Objetivo Legítimo debe limitar los poderes del Estado, no expandirlos

ARGENTINA: La Nueva Doctrina de Inteligencia Nacional resulta problemática y podría impulsar al Estado argentino a implementar prácticas que pueden significar la vulneración de los derechos humanos.[123] Esta Doctrina identifica varios objetivos legítimos para la vigilancia de inteligencia, pero lo hace con tal amplitud que parece expandir los estándares constitucionales, más que restringirlos. Asi mismo, Indica que las agencias de inteligencia se deben enfocar en la recopilación de información de un conjunto de cuestiones relativas a la defensa y seguridad nacional.

La definición de seguridad nacional que brinda esta nueva doctrina es ambigua: "fenómenos delictivos violatorios de las libertades y derechos de las personas y del Estado constitucional social y democrático de derecho".[124] Particularmente, establece que las actividades de inteligencia en este contexto deben abordar problemáticas como el terrorismo y la delincuencia organizada, con especial atención al narcotráfico y a la trata de personas. Entre las actividades de inteligencia que autoriza se encuentra el monitoreo de las comunicaciones vinculadas a "los atentados contra el orden constitucional y la vida democrática".

Según esta doctrina, se incluye en este grupo de actividades a las realizadas por grupos económicos o financieros que provoquen corridas bancarias y desabastecimientos que resulten en "golpes de mercado". Esta autorización puede fácilmente ser conflictiva, debido

123 Daniela Schnidrig y Verónica Ferrari, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina", *Centro de Estudios en Libertad de Expresión y Acceso a la Información, y Electronic Frontier Foundation,* (marzo de 2016). https://necessaryandproportionate.org/country-reports/argentina

124 Argentina, Decreto No. 1311/15, Boletín Oficial del 6 de julio de 2015, anexo 1.

a que va más allá de la definición de "actos de fuerza contra el orden institucional y el sistema democrático" que brinda la Constitución Nacional. Tal y como previene la Asociación por los Derechos Civiles, esto podría "podría incentivar prácticas estatales que podrían derivar en la violación de derechos de la ciudadanía. Los atentados al orden constitucional se encuentran claramente definidos en la Constitución y el poder ejecutivo no debería ampliar esos supuestos por vía reglamentaria".[125] Como se ha mencionado antes, a pesar que hubo un giro presidencial en Diciembre del 2015, la nueva administración no ha revocado expresamente la Nueva Doctrina ni la ha reemplazado con un documento similar.

El marco de telecomunicaciones argentino también vulnera el Principio de Objetivo Legítimo:[126]

> *En cuanto al marco de telecomunicaciones, las obligaciones de retención de información por los prestadores de servicios no se encuentran debidamente justificadas.*[127] *Tampoco justifica debidamente con qué fines.*
>
> *En materia de telecomunicaciones tampoco se cumple con este principio. Esta norma obliga a los usuarios a permitir el acceso de la autoridad de aplicación a los fines de realizar "todo tipo de trabajo o verificación necesaria" sin dar precisiones sobre qué tipo de trabajo, qué tipo de verificación y con qué fines.*[128] *También obliga a los prestadores de servicios de conexión móvil a informar a la autoridad sobre "toda información" sobre los usuarios y clientes del servicio sin dar cuenta cabalmente en el texto de la ley de cuáles serían los fines que justifican este tipo de medidas.*[129]

2.4 Garantías contra la discriminación

La legislación que autoriza medidas de vigilancia debe estipular que las actividades de inteligencia no deben usarse con fines discriminatorios. Muchas de las leyes cumplen con esto.

ARGENTINA: Favorablemente, la ley especifica que las agencias de inteligencia no pueden almacenar información por razones de raza, religión, acciones privadas, actividades políticas

125 Asociación por los Derechos Civiles, *Apuntes sobre el Decreto 1311/15*, pág. 2 (2015). http://www.adc.org.ar/wp-content/uploads/2015/07/Apuntes-sobre-el-decreto-1311-15.pdf.

126 Daniela Schnidrig y Verónica Ferrari, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina", *Centro de Estudios en Libertad de Expresión y Acceso a la Información, y Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/argentina

127 Argentina, Secretaría de Comunicaciones, art. 8.

128 Argentina, Ley 27.078 Argentina Digital, art. 60, sección D.

129 Argentina, Ley 25.891 sobre Servicios de Comunicaciones Móviles, art. 8.

o afiliaciones.[130]

COLOMBIA: Afortunadamente, la ley contiene una extensa lista de criterios que no pueden usarse para justificar actividades de vigilancia. Entre estos se encuentran: género, raza, origen nacional o familiar, idioma, religión, opinión política o filosófica, afiliación a organizaciones sindicales, sociales o de derechos humanos, o que promuevan los intereses de cualquier partido o movimiento político, o que afecte los derechos y garantías de partidos políticos de oposición.[131]

CHILE: La ley estipula que se pueden llevar a cabo ciertos procedimientos (que en Chile se llaman "procedimientos especiales de obtención de información") con el único fin de resguardar la seguridad nacional y proteger a Chile y a su pueblo de amenazas relacionadas con el terrorismo, la delincuencia organizada, y el narcotráfico.[132] Debería aclararse explicitamente que no se puede recurrir a la vigilancia con propósitos discriminatorios.

130 Argentina, Ley 25.520 de Inteligencia Nacional, Boletín Oficial del 6 de diciembre de 2001, art. 16f, incorporado por la Ley 27.126, art. 15

131 Colombia, Ley 1.621 de 2013, art. 4.

132 Chile, Ley 19.974, art. 23.

3.
Necesidad, Idoneidad, y Proporcionalidad

El Principio de Necesidad exige que todas las leyes de vigilancia, reglamentos y actividades estén limitados a lo estricta y evidentemente necesario para alcanzar un Objetivo Legítimo. La vigilancia sólo debe llevarse a cabo cuando es el único medio para lograr un objetivo legítimo, o cuando, habiendo varios medios, sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación recae siempre en el Estado.

El Principio de Idoneidad estipula que la vigilancia de las comunicaciones autorizada por ley debe ser un medio efectivo para cumplir el Objetivo Legítimo identificado.

El Principio de Proporcionalidad exige que la vigilancia de comunicaciones se considere un acto altamente intrusivo que interfiere con los derechos humanos y amenaza los cimientos de una sociedad democrática. Las decisiones sobre la vigilancia de las comunicaciones deben tener en cuenta la sensibilidad de la información accesible y la gravedad de la violación de los derechos humanos y otros intereses en cuestión, caso por caso.

Esta evaluación requiere que un Estado, como mínimo, demuestre que:

1. Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo;

2. Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la Información Protegida;[133]

133 Los 13 Principios definen a la información protegida como toda "información que incluye, refleja, surge de, o se refiere a las comunicaciones de una persona y que no está fácilmente disponible y accesible para el público en general. Tradicionalmente, el carácter invasivo de la Vigilancia de las Comunicaciones ha sido evaluado sobre la base de las categorías artificiales y formalistas. Los marcos legales existentes distinguen entre "contenido" o "no contenido", "información del suscriptor" o "metadatos", datos almacenados o datos en tránsito, datos que se tienen en el hogar o en la posesión de un tercero proveedor de servicios. Sin embargo, estas distinciones ya no son apropiadas para medir el grado de intromisión que la Vigilancia de las Comunicaciones realiza en la vida privada y las relaciones de las personas. Aunque desde hace tiempo se ha acordado que el contenido de la comunicación merece una protección significativa en la ley debido a su capacidad de revelar información sensible, ahora está claro que existe otra información que surge de las comunicaciones, y datos que no son contenido, que puede revelar incluso más acerca de una persona que el contenido en sí, y por lo tanto merece una protección equivalente. Hoy en día, cada uno de estos tipos de información, por sí sola o analizada colectivamente, puede revelar la identidad de una persona, su comportamiento, sus asociaciones, sus condiciones físicas o estado de salud, su

3. Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica;

4. La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza específica al fin legítimo alegado;

5. Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud;

6. La información será accedida solo por la autoridad específica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización; y,

7. Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

Estos principios deben evaluarse en las distintas etapas del proceso de vigilancia de las comunicaciones: evaluar la necesidad de la medida de vigilancia, la necesidad de retener información específica recopilada, y la posibilidad de que la medida de vigilancia haya tenido un impacto mínimo sobre la información protegida y los derechos humanos.[134]

Como indica la Guía universal para la implementación de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,[135] los agentes del gobierno que quieran llevar a cabo tareas de vigilancia para obtener información protegida:

[D]eben probar de manera clara que la vigilancia de las comunicaciones es el medio

raza, color, orientación sexual, origen nacional o puntos de vista, o puede permitir el mapeo de la ubicación de la persona, sus movimientos e interacciones en el tiempo, o puede hacer esto respecto de todas las personas en una ubicación determinada, incluyendo una manifestación pública u otro acontecimiento político. Como resultado, toda la Información Protegida debe recibir la máxima protección de la ley". Necessary and Proportionate Coalition, *Necessary & Proportionate*, (2014). http://necessaryandproportionate.org/principles *Vea* Necessary and Proportionate Coalition, *Necessary & Proportionate Global Legal Analysis*, (2014). http://necessaryandproportionate.org/global-legal-analysis

134 Access Now, "Guía universal para la implementación de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones" [Universal Implementation Guide For The International Principles On The Application Of Human Rights To Communications], (2015). https://en.necessaryandproportionate.org/files/2016/04/01/implementation_guide_international_principles_2015.pdf

135 Access Now, "Guía universal para la implementación de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones" [Universal Implementation Guide For The International Principles On The Application Of Human Rights To Communications], (2015). https://necessaryandproportionate.org/files/2016/04/01/implementation_guide_international_principles_2015.pdf

menos intrusivo que puede usarse para alcanzar el Objetivo Legítimo. [...] [N]o es suficiente que la vigilancia de las comunicaciones esté relacionada con el sujeto, el Objetivo Legítimo, la cuenta, dispositivo o archivo por registrar [...] sino que el [agente del gobierno] debe ceñir [su solicitud] para minimizar el impacto sobre otra información protegida.

Todas las solicitudes para llevar a cabo actividades de vigilancia de las comunicaciones deben explicar cuál es el Objetivo Legítimo de éstas, y la información exacta que se necesita para lograr ese Objetivo Legítimo. La solicitud también debe explicar por qué es necesario llevar a cabo la vigilancia de las comunicaciones y acceder a información personal y privada. Asimismo, debe identificar, tanto como sea posible, a quién/qué está dirigida la vigilancia de las comunicaciones.

Finalmente, el pedido debe describir detalladamente el alcance de la vigilancia de las comunicaciones solicitada. Una descripción adecuada de este alcance debe incluir la cuenta, dispositivo o archivo que estará bajo vigilancia, la base de datos particular correspondiente, toda información protegida externa a la cual se espera tener acceso, la metodología por usar, la importancia de la información necesaria para el Objetivo Legítimo identificado, y el cronograma específico, ya sea del periodo de tiempo en el que se adquirirán los datos, o el lapso durante el cual se tendrá acceso a una determinada cuenta, dispositivo o archivo.[136]

Una vez más, en América Latina, los Principios de Necesidad, Idoneidad y Proporcionalidad se reflejan tradicionalmente en los tratados internacionales de derechos humanos que cada Estado ratificó y reconoció en su constitución.[137] De hecho, los intereses que protegen estos Principios están profundamente incorporados en las constituciones de la región. Los Estados también adoptaron disposiciones legales que restringen los tipos de comunicaciones que pueden ser objeto de vigilancia. Sin embargo, el desarrollo de las nuevas tecnologías de vigilancia y la creciente cantidad de datos que se pueden obtener mediante la vigilancia de las comunicaciones complicaron la aplicación de estos Principios, lo que tuvo como consecuencia la carencia de Necesidad, Idoneidad y Proporcionalidad en las prácticas de vigilancia estatales.

La siguiente sección brinda algunos ejemplos interesantes de disposiciones legales destinadas a limitar el uso de la vigilancia de las comunicaciones a lo que es estrictamente idóneo y

136 Necessary and Proportionate Coalition, *Necesarios & Proporcionados*, (2014). http://necessaryandproportionate.org/principles; Necessary and Proportionate Coalition, *Necessary & Proportionate Global Legal Analysis*, (2014). http://necessaryandproportionate.org/global-legal-analysis

137 Valentina Hernández y Juan Carlos Lara, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile," *Derechos Digitales y Electronic Frontier Foundation*, (2016). https://necessaryandproportionate.org/country-reports/chile

proporcionado. En esta sección no expondremos una comparación detallada de la proporcionalidad de las reglas para las escuchas telefónicas. Se puede encontrar un análisis detallado sobre esa cuestión en los reportes nacionales de cada país. Tampoco examinamos en esta sección la manera en que se aplican estas leyes. Dicho estudio se encuentra, en gran parte, en el análisis del Principio de Legalidad, mencionado anteriormente. No obstante, sí brindamos un breve análisis de la proporcionalidad de las leyes de retención de datos, debido a que son inherentemente desproporcionadas.

3.1 La vigilancia de las comunicaciones debe limitarse a las situaciones en las que sea necesaria, idónea, y proporcionada

Algunos países de la región cuentan con leyes de vigilancia que tienen una redacción prometedora, aunque queda por ver si se implementan de una manera privada y protectora. Otros países limitan la vigilancia a los medios menos invasivos. Muchas leyes cumplen con algún aspecto de la proporcionalidad al establecer la duración máxima de las órdenes de vigilancia. Lo más alarmante es que las leyes de algunos países implementaron aparentemente estos Principios de Necesidad y Proporcionalidad, pero de tal manera que las leyes se vieron debilitadas.

EL SALVADOR: El artículo 2 de la Ley Especial para la intervención de las telecomunicaciones incorpora un análisis de proporcionalidad riguroso. Define a la vigilancia como un medio excepcional al que sólo se podrá recurrir si resulta útil para una investigación penal. Sin embargo, su necesidad debe justificarse de manera suficiente, y debe ser la medida menos gravosa para la investigación del crimen.

Esta ley también crea el Principio de Temporalidad, en el que toda intervención se mantendrá durante el tiempo que autorice el juez. La ley define correctamente a la intervención como la acción en la que una autoridad escucha, capta o registra una comunicación privada sin el consentimiento de sus participantes. Gracias a su redacción, la ley que regula la interceptación de las comunicaciones de El Salvador es prometedora, ya que favorece la privacía y secrecía de las comunicaciones.[138] Queda por ver si la ley se aplica de manera protectora y privada.

BRASIL: La Ley de Interceptación Telefónica 9.296 de 1996 usa un lenguaje prometedor en la teoría, pero es amplio en la práctica. El artículo 1 expandió el alcance de la regulación más allá de la interceptación telefónica e incluye "la interceptación de las comunicaciones que fluyen a través de los sistemas de informática y telemática".

> *[E]n la controversia sobre la interpretación correcta de la disposición constitucional que protege la confidencialidad de las comunicaciones, se impugnó su*

138 El Salvador, Ley Especial para la intervención de las telecomunicaciones, art. 3.

constitucionalidad en razón de que solo el flujo de comunicaciones telefónicas, y no cualquier otro tipo de comunicación, puede ser interceptado con limitación a que se use con los propósitos de una investigación penal. No obstante, la [Acción Directa de Inconstitucionalidad] fue desestimada por cuestiones procesales. Actualmente, el artículo 7, apartado II, del Marco Civil Da Internet, también permite la interceptación del flujo de las comunicaciones realizadas a través de Internet, mediante orden judicial, "como dicta la ley" (con referencia a la Ley de Interceptación).

La interceptación del flujo de las comunicaciones ocurre, conforme a las disposiciones de la cláusula principal del artículo 1 de la Ley 9.296/96, con el propósito de asistir en una investigación penal o hallazgo en un proceso penal, mediante orden judicial, sua sponte ("ex officio") o bajo la solicitud de un oficial de aplicación de la ley o de la Fiscalía General. [...] [E]stá prohibida la interceptación solicitada por autoridades que no hayan sido designadas de manera expresa, como la [...] ABIN".[139]

El artículo 2 de esta ley no admite la interceptación de comunicaciones en los siguientes casos: cuando no existen pruebas razonables de responsabilidad criminal o conspiración para la comisión de un crimen; cuando la evidencia puede obtenerse por otros medios; o cuando el hecho investigado no conlleva una pena mayor a la del tipo "*detenção*".[140] Los artículos 2, 4, y 5 indican que la interceptación de las comunicaciones puede tener lugar si está justificada:

[U]na solicitud de interceptación debe estar apoyada por una descripción clara de qué está bajo investigación, inclusive el nombre y la identificación de los sujetos, a menos que esto sea verdaderamente inviable. La solicitud deberá especificar los motivos de la investigación y los medios que se utilizarán", lo cual quedará establecido en la orden judicial.[141]

---

139 Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

140 Brasil, Ley 9.296 de 1996, art. 2. Fragmento de Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

141 Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazilDennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

[E]l periodo máximo de tiempo de interceptación es 30 días. La jurisprudencia imperante[142] *sostiene que una orden de interceptación puede ser prorrogada por tanto como se requiera. [...] El artículo 8 exige que los registros de las interceptaciones se manejen con confidencialidad, y el artículo 9 exige que se destruyan en el caso de que no sean útiles, o dejen de serlo para los propósitos probatorios.*[143]

GUATEMALA: Otra disposición alentadora se puede encontrar en el artículo 50 de la Ley contra la Delincuencia Organizada, que exige que la solicitud para interceptar comunicaciones incluya una justificación para su uso, junto con una explicación de la necesidad e idoneidad de la investigación:

Las solicitudes de autorización para la interceptación de las comunicaciones reguladas en la presente Ley, deberán presentarse por escrito ante el juez competente con los siguientes requisitos:

a) Descripción del hecho que se investiga, indicando el o los delitos en que se encuadran los mismos;

b) Números de teléfonos, frecuencias, direcciones electrónicas, según corresponda, o cualesquiera otros datos que sean útiles para determinar el medio electrónico o informático que se pretende interceptar [...];

c) Descripción de las diligencias y medios de investigación que hasta el momento se hayan realizado;

d) Justificación del uso de esta medida, fundamentando tanto su necesidad como su idoneidad; y

e) Si se tuvieren, nombres y otros datos que permitan identificar a la persona o personas que serán afectadas con la medida.

El artículo 51 brinda una definición para la "necesidad e idoneidad de la investigación":

Se entenderá que existe necesidad de la interceptación de las comunicaciones cuando los medios de investigación realizados demuestren que en los delitos

142 *Vea* Juez Joaquim Barbosa, Corte Suprema Federal, habeas corpus 84.301, sentencia del 9 de noviembre de 2004. (http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79542, y Juez Nelson Jobim, habeas corpus 83.515-RS, sentencia del 16 de septiembre de 2005. http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79377

143 Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y Protección de los Derechos Fundamentales", *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

cometidos por miembros de grupos delictivos organizados se estén utilizando los medios de comunicación establecidos en la presente Ley. [E]xiste idoneidad del uso de la interceptación de las comunicaciones cuando, atendiendo a la naturaleza del delito, se puede determinar que la interceptación de las comunicaciones es eficaz para obtener elementos de Investigación que permitan evitar, interrumpir o esclarecer la comisión de los delitos ejecutados por miembros de grupos delictivos organizados.

La normativa internacional de derechos humanos define a la "necesidad" de manera diferente. Debemos interpretar esta disposición teniendo en cuenta tanto a la Constitución como a los tratados internacionales de derechos humanos a los cuales suscribe el gobierno de Guatemala.

El artículo 51 de la Ley contra la Delincuencia Organizada afirma que la interceptación de las comunicaciones es un medio efectivo para la recolección de evidencia en la lucha para detener la comisión de crímenes llevados a cabo por grupos de delincuencia organizada. Esta misma ley también incluye una disposición legal favorable: la destrucción de los registros de vigilancia debe llevarse a cabo frente a un juez, una vez concluido el caso. La solicitud judicial para la interceptación de las comunicaciones debe contener una descripción de las diligencias y los medios de investigación que se hayan realizado hasta el momento.[144]

HONDURAS: Honduras cuenta con un modelo mixto. El artículo 5 de la Ley Especial sobre la Intervención de las Comunicaciones permite la vigilancia de las comunicaciones para cualquier crimen, con la condición de que no existan medidas de intervención menos onerosas.[145]

El artículo 6 establece que la interceptación de las comunicaciones puede tener lugar solamente durante investigaciones penales, y el Ministerio Público o la Procuraduría General deben establecer de manera razonable que existe un crimen cometido, en curso, o a punto de cometerse.

La solicitud de intervención debe contener cualquier información que se conozca sobre la persona cuyas comunicaciones serán objeto de vigilancia. Si se desconoce la identidad del individuo, la solicitud debe explicar las circunstancias bajo las cuales se solicita la investigación y brindar elementos básicos sobre la identificación de la persona (artículo 9). La solicitud también debe incluir información sobre los dispositivos de vigilancia que serán

144 Guatemala, Ley contra la Delincuencia Organizada, art. 50, Ministerio de Gobernación, (2006). http://leydeguatemala.com/ley-contra-la-delincuencia-organizada/requisitos-de-la-solicitud-de-autorizacion/10470/

145 República de Honduras, *Ley Especial sobre la Intervención de Comunicaciones Privadas*, Decreto No. 243-2011, (2011). http://www.conatel.gob.hn/doc/Regulacion/leyes/Ley_especial_comunicaciones_privadas.pdf

usados e información que pueda identificar a la persona bajo vigilancia, como su número de teléfono o dirección de correo electrónico (artículo 9).

También debe especificar la duración de la medida de vigilancia (artículo 9). La medida autorizada no deberá exceder los tres meses. Sin embargo, puede extenderse por otros tres meses, según la ley especial (artículo 12). Esta ley dicta de manera explícita que cuando el objetivo se haya cumplido, o cuando resulte inapropiado, innecesario, desproporcional o inviable, la vigilancia debe detenerse a solicitud del fiscal o el juez que haya emitido la autorización (artículo 16).

COLOMBIA: La legislación de Colombia que regula las actividades de inteligencia estipula explícitamente que dichas actividades deben estar regidas por el Principio de Necesidad. El artículo 5 de la Ley 1.621 de 2013 estipula: "La actividad de inteligencia y contrainteligencia debe ser necesaria para alcanzar los fines constitucionales deseados; es decir que podrá recurrirse a ésta siempre que no existan otras actividades menos lesivas que permitan alcanzar tales fines".

La legislación de Colombia también incorpora el Principio de Idoneidad cuando se trata de realizar tareas de inteligencia. El artículo 5 de la Ley 1.621 de 2013 establece:

> *La actividad de inteligencia y contrainteligencia debe hacer uso de medios que se adecúen al logro de los fines definidos en el artículo 4 de esta ley; es decir que se deben usar los medios aptos para el cumplimiento de tales fines y no otros.*[146]

El artículo 5 también contempla el Principio de Proporcionalidad en las operaciones de las agencias de inteligencia, e indica:

> *La actividad de inteligencia y contrainteligencia deberá ser proporcional a los fines buscados y sus beneficios deben exceder las restricciones impuestas sobre otros principios y valores constitucionales. En particular, los medios y métodos empleados no deben ser desproporcionados frente a los fines que se busca lograr.*

Además, el Decreto Legislativo 1.141 prevé que las actividades de inteligencia pueden ser solicitadas únicamente por el director de inteligencia nacional, y que tal solicitud debe contener: (i) la identificación de la(s) persona(s) afectada(s) por la medida; (ii) la descripción de las medidas solicitadas; y (iii) la justificación y duración de dichas medidas.

CHILE: El artículo 222 del Código Procesal Penal regula la interceptación telefónica y de otras telecomunicaciones:[147]

---

146 El artículo 4 se abordó en la sección sobre el Principio de Objetivo Legítimo.

147 Extracto del reporte de vigilancia en Chile, Valentina Hernández y Juan Carlos Lara, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile", *Derechos Digitales y Electronic Frontier Foundation* (2016).

En tal disposición se indica que en caso de existir fundadas sospechas, basadas en hechos determinados, 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 (es decir, que la pena asignada al delito sea de, al menos, cinco años y un día de prisión), y la investigación lo hiciere imprescindible, el juez de garantía, a petición del Ministerio Público, podrá ordenar la interceptación y grabación de este tipo de comunicaciones.

El requisito de las "fundadas sospechas" se refiere a que derivado de las circunstancias específicas del caso y hechos concretos que merezcan pena de crimen, se pueda argumentar que existe la creencia que la persona investigada ha participado en la preparación o comisión del delito o que lo hará. Igualmente, se establece un requisito de necesidad para la procedencia de la medida: que la medida sea imprescindible para el curso de la investigación.[148]

Como requisito previo a la autorización de la interceptación de las comunicaciones, el juez de garantía debe evaluar la necesidad de la interceptación de las comunicaciones para los efectos del proceso penal.

La legislación aplicable no hace mención específica a estos principios, pero ello se subentiende. Así, por ejemplo, en relación con el señalado artículo 222 del Código Procesal Penal, los límites temporales de la medida intrusiva, que se acote su margen a sólo los datos estrictamente necesarios o a los soportes que los contienen, que se acredite un cierto nivel de probabilidad ("fundada sospecha"), [...] y la exigencia de una pena mínima o una calificación especial atribuible a la conducta criminal desplegada, delimitan la procedencia de tales medidas, acotando lo que puede ser interceptado y registrado. [...]

El Principio de Necesidad se ve implícitamente recogido al enunciarse que el juez de garantía autorizará tales diligencias en caso de que la investigación del hecho lo hiciere imprescindible. Nuevamente, en la normativa sobre interceptación de comunicaciones es posible ver cada uno de ellos contemplados y efectivamente aplicados por la intervención del juez de garantía.[149]

Chile está entre los Estados que incorporan algún aspecto del Principio de Proporcionalidad en su legislación estableciendo periodos de tiempo máximos en las órdenes de vigilancia. La

---

https://necessaryandproportionate.org/country-reports/chile

148 Valentina Hernández y Juan Carlos Lara, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile", *Derechos Digitales y Electronic Frontier Foundation* (2016). https://necessaryandproportionate.org/country-reports/chile

149 Valentina Hernández y Juan Carlos Lara, "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile", *Derechos Digitales y Electronic Frontier Foundation* (2016). https://necessaryandproportionate.org/country-reports/chile

interceptación de comunicaciones para la investigación de un delito común puede autorizarse solamente por un periodo de 60 días; las comunicaciones relacionadas con el narcotráfico pueden interceptarse por 120 días, con órdenes renovables por periodos de 60 días.

La legislación sobre inteligencia de Chile también recoge el Principio de Necesidad en su redacción. El artículo 23 de la Ley 19.974 establece: "Cuando determinada información sea estrictamente indispensable para el cumplimiento de los objetivos del Sistema y no pueda ser obtenida de fuentes abiertas, se podrá utilizar los procedimientos especiales de obtención de información a que se refiere el presente Título, en la forma y con las autorizaciones que en el mismo se disponen". Los procedimientos especiales esbozados en el artículo 24:

a) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas;

b) La intervención de sistemas y redes informáticos;

c) La escucha y grabación electrónica incluyendo la audiovisual; y,

d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.[150]

La ley de Chile respeta también el Principio de Proporcionalidad, ya que detalla que los procedimientos de inteligencia especiales mencionados en el artículo 24 de la Ley 19.974, que tienen el potencial de vulnerar seriamente el derecho a la privacidad, están confinados a las tareas de inteligencia que tengan como objetivo resguardar la seguridad nacional y proteger a Chile y a su pueblo de amenazas relacionadas con el terrorismo, la delincuencia organizada, y el narcotráfico.[151] Una vez más, estas amplias definiciones de crímenes crean oportunidades para el abuso.

PERÚ: La ley peruana exige que toda la información de inteligencia obtenida por el Sistema de Inteligencia Nacional (SINA) que sea privada e innecesaria para los objetivos del Sistema debe ser destruida por los funcionarios correspondientes, bajo responsabilidad de inhabilitación y sin perjuicio de las sanciones civiles y/o penales que correspondan.[152]

Asimismo, la legislación peruana establece que todas las personas naturales o legales tienen la obligación de cooperar con el Sistema de Inteligencia Nacional (SINA) brindando toda información relativa a las investigaciones de inteligencia que sea requerida por el ente rector del sistema, en forma gratuita.[153] El mismo artículo estipula que cuando la información solicitada esté protegida por algún deber de reserva, la entrega de tal información no violará

150 Chile, Ley 19.974, art. 24.
151 Chile, Ley 19.974, art. 23.
152 Perú, Decreto Legislativo 1.141, art. 35.
153 Perú, Decreto Legislativo 1.141, art. 41.

esta obligación, ya que continuará bajo ese principio, con el cual todo el personal de inteligencia se ve obligado a cumplir. Sin embargo, existen excepciones a esta obligación, incluida la información protegida por el secreto profesional, la intimidad personal y familiar, secreto bancario, reserva tributaria, y otras que ampare la Constitución.

ARGENTINA: En la legislación de Argentina podemos encontrar una disposición similar a la peruana.[154] La ley estipula que las organizaciones de inteligencia tienen prohibido diseminar la información obtenida durante el ejercicio de sus funciones y que dicha información no se puede divulgar, a menos que medie orden judicial.[155] Además, como lo aclarará el Principio de Autoridad Judicial Competente, las organizaciones de inteligencia no pueden autorizar de manera autónoma la interceptación de las comunicaciones.

Se debe solicitar una autorización judicial cuando se considere necesario llevar a cabo tales medidas. Si el juez emite esta autorización, el sistema legal argentino limita la medida por un lapso determinado. El periodo de tiempo se puede extender por 90 días más, como máximo, siempre y cuando esa extensión temporal sea indispensable para completar la investigación.[156]

3.2 Prohibición de vigilar ciertos tipos de comunicación

Varios Estados en la región poseen leyes que prohíben la interceptación de las comunicaciones en ciertas circunstancias. La excepción más común es la de las comunicaciones entre un abogado y su cliente.

PARAGUAY: Paraguay mantiene una lista de excepciones clara. No se puede llevar a cabo la interceptación de acusados o testigos que hayan sido exonerados de declarar por parentesco o confidencialidad, incluidos los abogados y médicos. La ley prohíbe la obtención de las anotaciones de los abogados, las historias clínicas, o información de familiares cercanos. Esto quiere decir que si estos testigos toman nota de las comunicaciones que mantuvieron con el acusado, el gobierno no puede vigilarlas. Esta limitación aplica solamente a las comunicaciones de los testigos a los que se les conceda la posibilidad de abstenerse de declarar.[157]

CHILE: Las comunicaciones entre los acusados y sus defensores, por lo general, no pueden

154 Argentina, Ley No. 25.520 de Inteligencia Nacional, Boletín Oficial del 6 de diciembre de 2001, art. 16f.

155 Argentina, Ley No. 25.520 de Inteligencia Nacional, Boletín Oficial del 6 de diciembre de 2001, art.16c.

156 Argentina, Ley No. 25.520 de Inteligencia Nacional, Boletín Oficial del 6 de diciembre de 2001, art. 19

157 Paraguay, Ley 1286-98, *Código Procesal Penal*, art. 198 y 200. https://www.imolin.org/doc/amlid/Paraguay/Paraguay_Código_Procesal_Penal.pdf.

ser objeto de interceptación, excepto en los casos en que el juez de garantía crea que el abogado puede tener responsabilidad penal en el asunto investigado y ordene específicamente la vigilancia. El juez incluirá toda la información justificativa en la orden.[158]

URUGUAY: La ley prohíbe de manera expresa la interceptación de las comunicaciones que se den entre las personas indagadas y sus defensores, y cualquier comunicación sobre cuestiones que no tengan relación con el objeto de la investigación.[159]

MEXICO: La autoridad judicial federal no autorizará la vigilancia de asuntos electorales, fiscales, comerciales, civiles, laborales, o administrativos. Tampoco podrá autorizar la vigilancia de las comunicaciones entre los detenidos y sus defensores.

COLOMBIA Y NICARAGUA: El Código Procesal Penal de Colombia[160] y el de Nicaragua[161] prohíben la interceptación de comunicaciones entre los acusados y sus defensores.

158 Chile, Ministerio de Transporte y Comunicaciones, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación, 2005.

159 Uruguay, Ley 18.494, Control y prevención de lavado de activos y financiamiento del terrorismo, art. 5. http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/UY/ley_18494.pdf

160 Colombia, Ley 904 de 2004, *Código Procesal Penal*, art. 235.

161 Nicaragua, Ley 406*, Código Procesal Penal*, (2001), La Gaceta 243 y 244 (2001). http://legislacion.asamblea.gob.ni/Normaweb.nsf/%28$All%29/5EB5F62901601 6CE062571A1004F7C62

4.
La Cultura Del Secreto y el Derecho a Saber

Los Estados deben ser transparentes sobre el uso y alcance de las leyes de vigilancia de las comunicaciones, reglamentos, actividades, poderes o autoridades.

Conocer "lo que el gobierno está tramando" es el primer paso para asegurar que se respete las libertades fundamentales de sus ciudadanos. La transparencia tiene especial importancia cuando las agencias de aplicación de la ley adoptan nuevas tecnologías con propósitos de seguridad nacional. Sin transparencia, la sociedad civil es incapaz de hacer responsable a los gobiernos por usar tecnologías de vigilancia sin controles, como los dispositivos para el seguimiento de la ubicación de teléfonos celulares y el malware. El secreto impide el escrutinio democrático y significativo de las leyes de vigilancia, lo que deja efectivamente a las agencias de inteligencia y de aplicación de la ley en el rol de legisladoras.

El Relator Especial de la ONU para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA instaron a que haya transparencia en los gobiernos:

> *[T]oda persona tiene derecho a acceder a información bajo el control del Estado. Este derecho incluye la información que se relaciona con la seguridad nacional, salvo las precisas excepciones que establezca la ley, siempre que estas resulten necesarias en una sociedad democrática. Las leyes deben asegurar que el público pueda acceder a información sobre los programas de vigilancia de comunicaciones privadas, su alcance y los controles existentes para garantizar que no puedan ser usados de manera arbitraria. En consecuencia, los Estados deben difundir, por lo menos, información relativa al marco regulatorio de los programas de vigilancia; [...] los procedimientos de autorización, de selección de objetivos y de manejo de datos (incluidos datos agregados sobre su alcance).*

Existen varios métodos que pueden usar los Estados (y las compañías de telecomunicaciones) para incrementar la transparencia con respecto a la vigilancia de las comunicaciones:

1. Los Estados podrían hacer pública la información sobre compras de tecnología de vigilancia que hayan efectuado;

2. Las leyes de acceso a la información podrían usarse para obtener registros gubernamentales adicionales. En América Latina, las ONG están comenzando a

utilizar estas leyes para aprender sobre la vigilancia en sus países.

3. Los Estados (y las compañías privadas) podrían emitir informes de transparencia con el objetivo de brindar información útil a los ciudadanos y usuarios.

4. Las compañías de telecomunicaciones podrían establecer pautas públicas para la aplicación de la ley: un conjunto de reglas describiendo las circunstancias bajo las cuales podrán o no entregar información a agencias de aplicación de la ley.

5. Los periodistas de investigación que reciben documentos o fuentes mediante informantes que describen las capacidades o los objetivos de los programas de vigilancia gubernamental podrían publicar sus hallazgos.

A pesar de que muchos gobiernos son capaces de vigilar a sus ciudadanos de manera unilateral, a menudo obligan a un tercero —compañías de telecomunicaciones— a hacer el trabajo de vigilancia por ellos. Los proveedores de telecomunicaciones, las compañías de Internet, y los PSI quedan, en la mayor parte, obligados a asistir a los gobiernos de una u otra forma: ya sea facilitand el acceso directo a los datos de los usuarios o a sus instalaciones, o entregándoles datos de usuarios específicos que soliciten los gobiernos de conformidad con la ley.

En los Estados Unidos, muchas compañías de telecomunicaciones emiten informes de transparencia en los que revelan la cantidad de solicitudes de datos de usuarios recibidas por parte del gobierno. Normalmente, estos informes corporativos de transparencia se dividen en categorías basadas en el tipo de solicitud recibida:

1. solicitudes del gobierno para eliminar contenido;

2. solicitudes del gobierno para conocer datos de usuarios;

3. solicitudes del gobierno sobre derechos de autor;

4. estadísticas sobre malware y la detección de ataques de suplantación de identidad (phishing), entre otros.

Algunas compañías también hacen pública la cantidad de solicitudes que atendieron y la cantidad que rechazaron. Este tipo de informe es limitado en los casos en los que las compañías le brindan al gobierno acceso directo y no supervisado a sus sistemas (como divisores ópticos en la red de fibra óptica), ya que desconocen el alcance o el volumen del acceso gubernamental.

Mientras que la publicación de informes de transparencia se ha convertido en una buena práctica en las industrias de telecomunicaciones e Internet, no es una práctica generalmente adoptada en América Latina: La presentación de informes de transparencia referido a la vigilancia de las comunicaciones, no es habitual.

La mayoría de las agencias de inteligencia latinoamericanas se formaron durante la Guerra Fría, cuando muchos países estaban bajo dictaduras y sus gobiernos operaban bajo una cultura de secreto para mantener el status quo.[162]

En resumen: Existe una verdadera cultura del secreto en la región con respecto a la vigilancia de las comunicaciones:

1. Como explicamos en la sección sobre el Principio de Legalidad, muchos gobiernos han utilizado leyes secretas para justificar sus prácticas de vigilancia.

2. A pesar de que los pedidos de acceso a la información permiten a las personas obtener información sobre las actividades de vigilancia de las comunicaciones llevadas a cabo por el gobierno (como por ejemplo en Brasil), muchos países clasifican como confidencial toda la información de inteligencia — incluyendo la relacionada con la vigilancia de las comunicaciones— y extienden el concepto de confidencialidad tanto como sea posible.

3. Los proveedores de servicios de Internet (PSI) latinoamericanos (a excepción de México, que adoptó reglas que obligan a las compañías a emitir informes de transparencia) mantienen completamente en secreto el uso de las herramientas de vigilancia: las autoridades de investigación no expiden informes anuales sobre cómo usan sus poderes de vigilancia.

A continuación se detallan las prácticas de transparencia que encontramos en el contexto de la vigilancia de las comunicaciones en la región.

MÉXICO: En 2014, la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) expandió de manera significativa el alcance de los poderes de vigilancia de las autoridades. También impuso más obligaciones para los proveedores de servicios de telecomunicaciones y los PSI, para que cooperen en temas relacionados con la vigilancia estatal de las comunicaciones (por ejemplo, el artículo 189 de la LFTR, con el propósito de establecer garantías relativas a la transparencia, exige que el Instituto Federal de Telecomunicaciones (IFT) expida "Lineamientos de Colaboración en Materia de Seguridad y Justicia".[163] El artículo 18 de estos lineamientos obliga a los servicios de telecomunicaciones y a las PSI que publiquen un informe semestral que incluya:

(i) El número total y por Autoridad Facultada, de requerimientos de información

162 Samanta Curti. "Reformas de los Sistemas de Inteligencia en América del Sur". http://www.kas.de/wf/doc/17940-1442-1-30.pdf

163 Instituto Federal de Telecomunicaciones. Lineamientos de Colaboración en Materia de Seguridad y Justicia. Publicados en el Diario Oficial de la Nación el 2 de diciembre de 2015. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

de localización geográfica en tiempo real y de registro de datos de comunicaciones, desglosando las recibidas, entregadas y no entregadas, (ii) el número de registros de datos de comunicaciones cancelados y suprimidos, una vez cumplido el fin para el cual fueron solicitados".[164]

Algunos PSI de México son los únicos que han publicado informes de transparencia, liderando en la región en este tema. Iusacell, Movistar, Nextel, y Telcel publicaron de manera conjunta informes mediante ANATEL (Asociación Nacional de Telecomunicaciones). Sin embargo, dichos informes a menudo no son lo suficientemente detallados. Según la EFF y la Red en Defensa de los Derechos Digitales, "sólo muestran un número genérico de solicitudes realizadas por las autoridades para la persecución de delitos, sin proporcionar información detallada sobre el tipo de solicitudes de datos que las compañías han recibido, qué instituciones de gobierno las formularon o qué razones fueron dadas por las autoridades para fundar estas solicitudes".[165]

Para afrontar la cuestión de la transparencia de agencias gubernamentales, México promulgó una Ley General de Transparencia y Acceso a la Información Pública en 2015. El artículo 70, apartado XLVII, de esta ley exige a las agencias federales que publiquen, con fines estadísticos, un listado de solicitudes realizadas a empresas concesionarias de telecomunicaciones para la intervención de comunicaciones privadas, el acceso a los registros de comunicaciones, y la localización geográfica en tiempo real de equipos de comunicación. Esta lista debe incluir el alcance y los fundamentos legales de las solicitudes, y especificar cuando la solicitud requiera autorización judicial. No obstante, la misma ley clasifica como información reservada cualquier información que pudiera poner en peligro la seguridad nacional, la seguridad pública o la defensa nacional (artículo 113). En el ámbito de la inteligencia, el artículo 51 de la Ley de Seguridad Nacional de México clasifica como información reservada "aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipos útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen".

BRASIL: La Resolución (*Resolução*) No. 59 de 2008 exige que los fiscales (incluyendo la policía) y los jueces informen al Inspector General de la Procuraduría y al Inspector General del Poder Judicial de la Nación, respectivamente, el número de operaciones de interceptación de comunicaciones en curso en el país. Deben entregar estos datos

164 Luis Fernando García, "México: Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en México", Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales (2016). https://necessaryandproportionate.org/country-reports/mexico

165 Informe "¿Quién Defiende Tus Datos?" Muestra Mucho por Hacer Para Defender la Privacidad de Usuarios de Internet en México, (2015) https://www.eff.org/deeplinks/2015/06/new-report-shows-which-mexican-isps-stand-their-users

mensualmente, a efectos estadísticos, y estos deben versar sobre las escuchas telefónicas y las interceptaciones de tecnologías de la información y telemática usadas en el Sistema Nacional de Control de Interceptaciones.

Estos datos no son de carácter público, pero están disponibles bajo solicitud. Por ejemplo, InternetLab,[166] mediante un pedido de Acceso a la Información, obtuvo la siguiente información: en promedio, se realizan escuchas telefónicas en 18.000 líneas y se envían 50.265 notificaciones de interceptación a las compañías de telecomunicaciones cada mes.[167]

URUGUAY: No existe regulación obligando a las agencias de inteligencia y de investigación penal a publicar datos sobre sus actividades de vigilancia.[168] Además, tampoco existe obligación para que los servicios de telecomunicaciones y los Proveedores de Servicio de Internet (PSI) publiquen estadísticas (información agregada) sobre las solicitudes que reciban por parte de las agencias de aplicación de la ley para interceptar las comunicaciones o acceder a los datos.[169]

Las autoridades reportaron al Parlamento sobre sus escuchas telefónicas y han respondido a algunas solicitudes específicas, pero no informan regular y sistemáticamente sobre otras de sus actividades de vigilancia. Por ejemplo, recientemente un candidato a presidente hizó un requerimiento de información para conocer si alguna agencia de investigación penal estaba interceptando sus comunicaciones. Dirigió el pedido a la Suprema Corte de Justicia uruguaya, la cual informó que se habían realizado un total de 6.150 escuchas telefónicas entre 2009 y 2014, sin contestar la pregunta específica del candidato.[170]

Uruguay necesita más transparencia con respecto a la compra de herramientas de vigilancia. Por ejemplo, las autoridades no explicaron bajo qué procedimiento adquirieron el software El Guardián;[171] esta información está clasificada como "reservada" bajo la Ley de Acceso a la Información. Además, la evidencia sugiere que existen decretos secretos que regulan los

166 InternetLab, http://www.internetlab.org.br/en/about/

167 Dennys Antonialli, Jacqueline de Souza Abreu, "Brasil: Vigilancia estatal de las comunicaciones en Brasil y la protección de derechos fundamentales", Electronic Frontier Foundation & InternetLab (octubre de 2015). https://necessaryandproportionate.org/country-reports/brazil

168 Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Uruguay: Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en Uruguay", Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/uruguay

169 Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Uruguay: Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en Uruguay", Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/uruguay

170 El País. "Jueces disponen de escuchas prudentemente" http://www.elpais.com.uy/informacion/jueces-disponen-escuchas-telefonicas-prudentemente.htm

171 Penumbra: Surveillance, security and public information in Uruguay, GISWatch (2014). http://www.giswatch.org/en/country-report/communications-surveillance/uruguay

procedimientos de conexión de los servicios de telecomunicaciones y los PSI a El Guardián. Como se indicó anteriormente, las autoridades deberían divulgar las leyes —y decretos— bajo las que operan las agencias de inteligencia, a los fines de rendición de cuentas.[172]

CHILE: La Ley General de Transparencia de Chile aplica a la mayor parte de las agencias estatales, incluyendo toda la rama judicial y la Fiscalía General (Ministerio Público).[173] Según esta ley, los ciudadanos chilenos pueden solicitar estadísticas de vigilancia y demás información, a menos que los datos no pueden ser revelados debido a razones de seguridad nacional. El artículo 38 de la Ley 19.974 del año 2004, que regula la estructura general de la inteligencia chilena, clasifica toda la información de inteligencia nacional y la información recopilada por los funcionarios públicos de agencias de inteligencia como reservada y secreta.[174] El informe anual del Ministerio Público no revela la cantidad de "interceptaciones de comunicaciones han sido ordenados cada año.[175]

ARGENTINA: No existen obligaciones legales para la entrega de informes de transparencia sobre la interceptación de las comunicaciones por cuestiones penales en este país. Por otra parte, las agencias de inteligencia están obligadas a entregar anualmente informes confidenciales sobre sus actividades de inteligencia a la Comisión Bicameral de Fiscalización de Organismos y Actividades de Inteligencia.[176]

En Septiembre de 2016, la Cámara de Diputados de Argentina aprobó la Ley de Acceso a la Información Pública y la convirtió en ley.[177] La Casa de Representantes insistió con su versión del proyecto de ley después que el Senado introdujera cambios el 7 de Septiembre del 2016. La nueva ley permite a los argentinos solicitar información a la Fiscalía General, y cualquier juez del Poder Judicial.[178] Sin embargo, esta ley contiene excepciones de seguridad

172 Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Uruguay: Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en Uruguay", Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/uruguay

173 República de Chile. Ley de Transparencia. http://www.leychile.cl/Navegar?idNorma=276363

174 Ley 19.974 (2004). http://www.interior.gob.cl/transparencia/ani/

175 Juan Carlos Lara, "Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en Chile", Derechos Digitales y Electronic Frontier Foundation (2016). https://necessaryandproportionate.org/country-reports/chile

176 Verónica Ferrari and Daniela Schnidrig, "Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en Argentina", marzo de 2016, Centro de Estudios en Libertad de Expresión y Acceso a la Información, y Electronic Frontier Foundation.https://necessaryandproportionate.org/country-reports/argentina

177 Télam. La Cámara de Diputados Aprobó la ley de Acceso a la Información Pública. September 14, 2016. Available at: http://www.telam.com.ar/notas/201609/162990-camara-de-diputados-acceso-a-la-informacion.html.

178 Republic of Argentina. Draft Bill for Access to Public Information. Article 7. "Proyecto de ley de Acceso a la Informacion Publica." http://www.saij.gob.ar/proyecto-ley-acceso-informacion-publica-enviado-al-congreso-poder-ejecutivo-nacional-proyecto-ley-acceso-

nacional; información no será proporcionada en circunstancias en las que una investigación criminal podría estar en peligro.[179]

PARAGUAY: Las leyes que regulan la vigilancia de las comunicaciones no exigen que el Estado publique informes de transparencia para las investigaciones penales ni para las operaciones de inteligencia nacional. Los informes anuales de la Policía Nacional, el Ministerio Público, y la SENAD (la Secretaría Nacional Antidrogas) no contienen el número de solicitudes aprobadas y rechazadas, ni tampoco el número de solicitudes realizadas por proveedores de servicios, autoridades, ni el tipo de solicitud y su propósito.[180]

Paraguay es único, en el sentido en que creó recientemente una agencia de inteligencia centralizada (2014)[181] y también aprobó una Ley de Acceso a la Información, que sólo aplica al Poder Judicial y a algunas partes del Ejecutivo, pero no a la nueva agencia de inteligencia centralizada.[182]

PERÚ: La legislación peruana no obliga a las agencias de inteligencia a publicar estadísticas sobre el número de solicitudes de interceptaciones de comunicaciones que se han enviado al Poder Judicial. Como consecuencia, hay una falta de información sobre la cantidad de autorizaciones judiciales que se han aprobado en el país. También falta transparencia en los procedimientos que regulan la vigilancia de las comunicaciones. En 2015, el gobierno peruano emitió la Resolución Ministerial 0631-2015-IN: "Protocolo para el mejor acceso a los datos de geolocalización de teléfonos móviles y dispositivos electrónicos de naturaleza similar". Establece el procedimiento para el acceso a los datos de geolocalización, según el Decreto Nº 1182. El Protocolo no está disponible al público; se categorizó como información clasificada, en virtud de la Ley de Libertad de Información.[183]

Con respecto al sector privado, los proveedores peruanos todavía no han adoptado el hábito de presentar informes de transparencia. En 2015, la ONG peruana Hiperderecho y la Electronic Frontier Foundation publicaron "¿Quién defiende tus datos?", un reporte que

---

informacion-publica-enviado-al-congreso-poder-ejecutivo-nacional-nv14182-2016-04-07/123456789-0abc-281-41ti-lpssedadevon

179 Ibid. Aricle 8.

180 Jorge Rolón Luna, Maricarmen Sequera, "Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en Paraguay", Electronic Frontier Foundation & TEDIC (marzo de 2016). https://necessaryandproportionate.org/country-reports/paraguay

181 Congreso de Paraguay aprueba agencia nacional de inteligencia tras ataques del EPP, Insight Crime, (2014) http://es.insightcrime.org/noticias-del-dia/congreso-de-paraguay-aprueba-agencia-nacional-de-inteligencia-tras-ataques-del-epp

182 República de Paraguay. Ley 5282. http://informacionpublica.paraguay.gov.py/public/ley_5282.pdf

183 ONG Hiperderecho. "Policía considera 'reservada' la forma en la que aplica la Ley Stalker" (2015). http://www.hiperderecho.org/2016/02/policia-ley-stalker-reservada-la-forma-en-la-que-aplica-la-leystalker

evaluó a los principales proveedores de Internet en Perú en relación con sus políticas de privacidad y prácticas de protección de datos. Ninguna de las compañías en el análisis proporcionó información concerniente a las solicitudes de datos que recibieron por parte del gobierno.[184]

Es por esto por lo que no hay información disponible públicamente, ni por parte del gobierno ni de los proveedores, sobre la cantidad de solicitudes que ha enviado el gobierno a los PSI para acceder a los datos retenidos.

EL SALVADOR: El artículo 10 de la Ley de Acceso a la Información Pública estipula que las estadísticas generadas por todas entidad estatal tienen carácter público, incluidas aquellas producidas por la Fiscalía General, que supervisa al Centro de Intervención a las telecomunicaciones.[185] Aun así, si bien la Fiscalía General publica algunas estadísticas sobre información de solicitudes en virtud de esta ley, los datos no son claros con respecto al tipo de entidad o individuo que solicita la información. Además, no se han publicado informes anuales sobre el número de solicitudes de vigilancia aprobadas y rechazadas.[186]

HONDURAS: La Ley de Libertad a la Información puede usarse para obtener información estadística sobre las solicitudes de vigilancia siempre y cuando los datos existan y no estén clasificados como confidenciales. Sin embargo, la información estadística que produce el Centro de Interceptaciones se considera confidencial (información reservada). Además, toda la información que produce el Centro de Intervenciones es clasificada como información de inteligencia confidencial.[187]

GUATEMALA: La ley nacional de Guatemala no exige la publicación de informes de transparencia sobre vigilancia, y la administración no publica esta información. No obstante, según el artículo 30 de la Constitución de Guatemala, todas las acciones de la administración son públicas. No queda claro, sin embargo, si una impugnación exitosa hacia esta secrecía del gobierno podría basarse en esa disposición.[188]

184 ONG Hiperderecho. Electronic Frontier Foundation. "¿Quién Defiende tus Datos?" (2015). http://www.hiperderecho.org/qdtd/

185 Ley de Acceso a la Información, http://www.fiscalia.gob.sv/wp-content/uploads/portal-transparencia/Ley-de-Acceso-a-la-Informacion-Publica.pdf

186 El Salvador. Fiscalía General. http://www.fiscalia.gob.sv/datos-estadisticos-de-solicitudes-recibidas-de-enero-mayo-de-2014/#/6/zoomed

187 Edy Tábora Gonzáles, Capítulo de Honduras. En: Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.). -- 1a. ed.-- San José, C.R.: Fundación Acceso, 2015. pdf; 4MB

188 Jorge Jiménez Barillas Hedme Sierra-Castro. Capítulo de Guatemala. En: Fundación Acceso, Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos

NICARAGUA: Nicaragua cuenta con una ley de acceso a la información (Ley 621 de 2001).[189] Sin embargo, esta ley clasifica como confidencial la información relativa a la seguridad nacional. No hay estadísticas disponibles acerca de la cantidad de solicitudes de interceptaciones que se han realizado.[190]

COLOMBIA: La Ley 1621 de 2013 no obliga a las agencias de inteligencia a informar cuántas interceptaciones de comunicaciones se llevan a cabo por año.[191] Si bien Colombia cuenta con una ley de transparencia (Ley 1712 de 2014: "Ley de Transparencia y Derecho a la Información Pública")[192] que obliga a las entidades públicas a publicar datos sobre sus actividades, la defensa y la seguridad nacional son excepciones a esta obligación.[193] Lo mismo ocurre con las solicitudes de información realizadas bajo el "derecho de petición" que recoge la Constitución, el cual habilita a los ciudadanos a solicitar información sobre cualquier agencia gubernamental. Además, la Ley de Inteligencia en Colombia indica de manera expresa que la supervisión de las actividades de inteligencia queda bajo estricta reserva.

Asimismo, los procedimientos penales están regulados por el principio de publicidad. Esto quiere decir que "las audiencias en las que se controla la legalidad de las interceptaciones de comunicaciones y otras medidas de vigilancia están abiertas al escrutinio público". Aun así, el artículo de la Ley 906 de 2004 estipula que el juez puede limitar la publicidad de los procedimientos si estima que publicarlos pondría en peligro la seguridad nacional.[194]

Desde el ámbito del sector privado, el año pasado, la Fundación Karisma y la Electronic Frontier Foundation publicaron de manera conjunta un reporte llamado "Colombianos a sus ISPs: ¿Dónde están mis datos?", en el que se detalla que ninguno de los PSI colombianos

---

humanos. Peri, Luciana (coord.), (San José, C.R.: Fundación Acceso, 2015).

189 República de Nicaragua, Ley 621 de 2007. http://www.oas.org/juridico/spanish/mesicic3_nic_ley621.pdf. Artículo 15.

190 Fundación Acceso, Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.), (San José, C.R.: Fundación Acceso, 2015).

191 República de Colombia, Ley 1621 de 2013, artículo 21.

192 República de Colombia, Ley 1712 de 2014. Artículo 9, artículo 11. http://www.centrodememoriahistorica.gov.co/descargas/transparencia/Ley1712-transparencia-acceso-informacion.pdf

193 En caso de duda sobre si la información es de carácter público o está sujeta a una de las excepciones, deberá prevalecer el criterio de Publicidad. República de Colombia, Ley 1712 de 2014. Artículo 5.

194 Juan Camilo Rivera y Katitza Rodriguez, "Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en Colombia", Comisión Colombiana de Juristas, la Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

publica informes de transparencia.[195]

En síntesis, los Estados de la región —a excepción de México— generalmente tienen un entorno legal defectuoso y poco claro en relación con la divulgación de la naturaleza, el alcance, o el propósito de las actividades estatales de vigilancia de las comunicaciones.

195 Electronic Frontier Foundation y Fundación Karisma. Colombianos a sus ISPs: "¿Dónde están mis datos?". https://www.eff.org/deeplinks/2015/05/which-internet-providers-tell-colombians-where-their-data

5.
Notificación del usuario

Si una autoridad tiene la facultad de vigilar las comunicaciones, la ley debe también reconocer el derecho de las personas a ser notificada acerca de tal vigilancia. Los individuos deben recibir una notificación de la decisión de autorizar la vigilancia de las comunicaciones con el tiempo y la información suficientes para que puedan impugnar la decisión o buscar otras soluciones, y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación sólo se justifica cuando el juez a cargo de emitir la autorización de la vigilancia determine que tal notificación pondría en peligro la finalidad para la que se autoriza la vigilancia, o cuando existiere un riesgo inminente de peligro para la vida humana. De igual manera, la ley debe fijar fechas límite para el aplazamiento de la notificación.

En algunas jurisdicciones (como Colombia y El Salvador), los acusados tienen el derecho a acceder a la evidencia originada mediante la vigilancia durante el juicio penal, con el objetivo de impugnar su legalidad o admisibilidad. Sin embargo, otras jurisdicciones también brindan un derecho a la notificación más amplio, en teoría, a aquellos afectados por la vigilancia, ya sea que los afectados se conviertan o no en los acusados en un proceso penal, una vez que la investigación sea completada. Este es el caso de Perú y Chile. Ningún estado prevé de manera clara la notificación antes de que se complete la vigilancia, incluso cuando la información se busca de manera retrospectiva (en comunicaciones pasadas) en vez de en comunicaciones futuras.

En el contexto de inteligencia, ningún estado de la región estableció medidas de notificación. Estas medidas son necesarias.

PERÚ: Perú cuenta con una mejor política de notificación que otros países de la región. En este país, la notificación del usuario ocurre solamente después del cierre de la investigación penal. Según el artículo 231 del Código Procesal Penal, una vez que las actividades de vigilancia y las investigaciones están terminadas, el individuo sometido a la vigilancia debe ser notificado de ello. Los afectados pueden exigir la reevaluación judicial de la vigilancia dentro de los tres días siguientes a haber recibido la notificación. No obstante, el Código deja en claro que los individuos bajo investigación no recibirán notificación cuando esta pueda poner en peligro la vida o integridad física de un tercero. Esta disposición es similar a la del Tribunal Europeo de Derechos Humanos en Ekimdzhiev vs. Bulgaria, en donde se indica que una vez acabada la vigilancia y transcurrido el tiempo necesario para que el

objetivo legítimo no esté en riesgo, los afectados deben ser notificados sin más dilación.[196]

A pesar de este principio general, las leyes de Perú sí restringen la notificación en al menos una situación de vigilancia: la ley prohíbe a los empleados de compañías revelar si la compañía tiene órdenes de recopilar datos telefónicos. Sin embargo, puede que esta restricción no aplique a la compañía en su totalidad. La zona gris se hace presente en la redacción del Código Procesal Penal que establece:

Artículo 230:

> *4. Las empresas telefónicas y de telecomunicaciones deberán posibilitar la diligencia de intervención y grabación o registro, bajo apercibimiento de ser denunciados por delito de desobediencia a la autoridad. Los encargados de realizar la diligencia y los servidores de las indicadas empresas deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento.*

CHILE: No se permite la notificación previa. El artículo 224 del Código Procesal Penal exige la notificación a los afectados por una medida de vigilancia, luego de que esta haya terminado, cuando el objetivo de la investigación lo permita, y no se ponga en peligro la vida o la integridad física de terceros. El artículo 182 exige la secrecía de la investigación pero permite que el acusado tenga acceso a la evidencia en su contra en un proceso penal.

MÉXICO: No existe obligación legal que exija al Estado o a las compañías notificar a los usuarios que estén sometidos a la vigilancia. La ley no aborda el caso de la notificación una vez concluida la investigación.

ARGENTINA: No existe mandato legal alguno obligando al Estado ni a las empresas a notificar a los usuarios que están siendo objeto de vigilancia. Al igual que en México, la ley no contempla la necesidad de notificación después de la conclusión de una investigación. No existe ningún mandato legal que ordene la notificación ni a las empresas ni a los servicios de inteligencia; ni siquiera a los fiscales que llevan a cabo una investigación o elevan las acusaciones. De facto, los usuarios pueden descubrir accidentalmente que han sido vigilados si el material resultante de la vigilancia se utiliza como prueba en un procedimiento penal. Pero no hay ninguna obligación, actualmente, que obligue a los funcionarios públicos a revelar el origen de las mismas.

Sin embargo, los usuarios tienen derecho a solicitar el acceso a la información recogida sobre ellos por las agencias de inteligencia. Este derecho ha sido reconocido por el Tribunal Supremo en la decisión *Ganora*, que establece que los funcionarios de inteligencia no

196 Tribunal Europeo de Derechos Humanos. Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria. Aplicación nº 62540/00. Sentencia del 28 de junio de 2007.

pueden argumentar una excepción generalizada, que les permita rechazar todas las solicitudes de acceso a la información realizadas por aquellas personas sobre su propia información. Por el contrario, el Tribunal Supremo sostuvo que si se aplica alguna excepción para acceder a esta información, debe entonces encontrarse justificada por las autoridades de inteligencia.[197] El Tribunal Supremo ratificó esta línea doctrinal en la decisión R. P., R. D. de 2011.[198]

BRASIL: No existe obligación legal que exija al Estado o a las compañías notificar a las personas que serán sometidas a la vigilancia antes de llevarla a cabo. Sin embargo, el Código Procesal Penal prevé que un juez, ante la presentación de una medida cautelar, como el pedido de una orden judicial, deberá notificar a los afectados, "excepto en los casos de emergencia o ante la posibilidad de comprometer la efectividad de la medida".[199]

Esta excepción se aplica rutinariamente a las investigaciones penales en curso. Cuando un caso penal entra en juicio, la ley únicamente garantiza que el acusado será notificado de la medida de vigilancia cuando los fiscales pretendan utilizar evidencia obtenida mediante ella (artículo 370, CPP).

Como explica el reporte sobre Brasil, "con respecto a los intermediarios, la mayoría de las solicitudes de datos y órdenes de escuchas están acompañadas de mordazas legales que prohíben a las compañías telefónicas y a los proveedores de servicios de Internet entregar la notificación. Sin embargo, aunque no existen órdenes mordaza con respecto a la notificación del usuario en otras circunstancias, las compañías no llevan a cabo esta práctica de manera proactiva."[200]

La ley no aborda los términos de notificación una vez concluida la investigación.

NICARAGUA: No existen obligaciones legales en el Código Procesal Penal ni en la Ley de Crimen Organizado que exijan al Estado o a las compañías notificar a los usuarios cuando estos sean sometidos a la vigilancia. El artículo 66 de la Ley de Crimen Organizado impone un "deber de confidencialidad" a todos aquellos que intervengan en la interceptación de las comunicaciones, el cual prohíbe cualquier tipo de divulgación, bajo pena de ley, salvo en el curso de la presentación de la evidencia en el proceso penal. Esta obligación no parece tener fecha de caducidad.

---

197 Supreme Court of Argentina. Ganora s/ hábeas corpus. Decision of September 16, 1999.

198 Supreme Court of Argentina. R.P, R.D. c/ Secretaría de Inteligencia. Decision of April 19, 2011.

199 Artículo 282, § 3.

200 Dennys Antonialli y Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y la Protección de los Derechos Fundamentales", Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

Art. 66: Deber de Confidencialidad

> *[S]alvo en lo que concierne a su incorporación en el proceso penal, las autoridades, funcionarios o empleados públicos, así como los particulares que intervengan en el procedimiento de intervención de las comunicaciones deberán guardar absoluta reserva de cuanto conozcan. La inobservancia de este deber será sancionado conforme al Código Penal.*

COLOMBIA: La ley garantiza que dentro del proceso penal, al momento de la audiencia, el acusado que está bajo vigilancia será notificado para que pueda impugnar la legalidad de la medida de vigilancia durante dicha audiencia. El artículo 15 del Código Procesal Penal indica que las partes tienen el derecho de objetar cualquier tipo de recopilación de la información. El Fiscal General puede recopilar evidencia mediante el uso de distintos métodos de interceptación de las comunicaciones sin el consentimiento del titular de estas. Dicha interceptación será validada por el juez de garantías constitucionales (quien analiza si la interceptación se ajusta a las garantías constitucionales y procesales). Este tipo de evidencia puede ser rechazada cuando no se ajuste a las garantías mencionadas. Por lo tanto, en la mayoría de los casos, la persona descubre que sus comunicaciones han sido interceptadas después de que la medida se lleva a cabo, pero durante el proceso penal.

En lo que respecta a los procedimientos de inteligencia, estas autoridades, en teoría, no están autorizadas para interceptar comunicaciones porque no son parte de la Policía Judicial (SIJIN) —la institución facultada que respalda al Fiscal General en la interceptación de las comunicaciones. La Ley de Inteligencia y Contrainteligencia no contiene obligaciones de notificación ya que, según esta ley, la interceptación de las comunicaciones queda relegada a las investigaciones penales.

La ley no prevé la notificación previa, ni la notificación una vez concluida la investigación, ni tampoco la notificación para las personas que no sean las acusadas.

EL SALVADOR: La Ley Especial para la Intervención de las Telecomunicaciones no exige, de manera específica que la persona afectada deba ser notificada sobre la decisión de autorizar la vigilancia. Sin embargo, el artículo 25 indica que "[u]na vez entregado el expediente judicial de la intervención del juez competente, el mismo será público, excepto que resulten aplicables las reglas generales de reserva del proceso penal". El artículo 26 establece que una vez incorporado el expediente judicial al proceso penal, "la defensa tendrá acceso completo e irrestricto al mismo".

La ley no prevé la notificación previa, ni la notificación una vez concluida la investigación, ni tampoco la notificación para las personas que no sean las acusadas.

HONDURAS: El marco legal no exige específicamente que se notifique a la persona afectada *a priori* sobre la decisión de autorizar la vigilancia. Sin embargo, el Código Procesal Penal incluye una obligación de notificación general de la diligencia investigativa solo después de la formulación de cargos en contra del sujeto. En los demás casos, no se exige la notificación. El artículo 21 de la Ley Especial sobre Intervención de las Comunicaciones Privadas también establece la confidencialidad del expediente legal (la reserva del expediente) durante el tiempo en el que transcurra la medida de vigilancia, y el expediente debe incorporarse en el archivo judicial principal una vez que esta haya cesado.[201]

La ley no prevé la notificación previa, ni la notificación una vez concluida la investigación, ni tampoco la notificación para las personas que no sean las acusadas.

201 Capítulo de Honduras. Edy Tábora Gonzales. Fundación Acceso, Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.).p. 228

6.
¿Quién Vigila a Quiénes Nos Vigilan?
Autoridad judicial competente y debido proceso

Los Principios de necesidad y proporcionalidad exigen que la vigilancia estatal de las comunicaciones sea autorizada caso por caso por una autoridad judicial que sea imparcial e independiente. Esto asegura que el Estado no actúe más allá de sus capacidades y que se les dé una debida consideración a los derechos humanos de aquellos que son afectados por la vigilancia. Esto garantiza que los derechos humanos del sujeto queden protegidos en cada paso del proceso de autorización. Al exigirle al Estado que justifique cada acto de vigilancia ante un juez, el principio asegura que la vigilancia de las comunicaciones se lleve a cabo únicamente cuando sea necesaria y cuando el costo hacia los derechos humanos sea inexistente o mínimo. También garantiza que, cuando sea posible, el sujeto de la vigilancia tenga la oportunidad de impugnar la acción que pretenda realizar el estado.

En la mayoría de los países, se les concede a los jueces el poder de autorizar la vigilancia de las comunicaciones en investigaciones penales. Sin embargo, los tribunales han emitido opiniones que variaron el grado de autorización judicial y debido proceso dependiendo de qué vigile el estado: el contenido de las comunicaciones, los datos de ubicación o la información del suscriptor. En algunos estados, la ley no exige autorización previa, o ni siquiera retroactiva, para acceder a los datos del suscriptor, la información de la ubicación, o los metadatos.

El Principio de Autoridad Judicial establece que la autoridad judicial de supervisión debe:

1. estar separada e independiente de las autoridades encargadas de la vigilancia de las comunicaciones;

2. estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la vigilancia de las comunicaciones, las tecnologías utilizadas y los derechos humanos; y

3. tener los recursos adecuados en el ejercicio de las funciones que se le asignen.

El Principio de Debido Proceso aborda muchas de las mismas preocupaciones y promueve muchas de las mismas políticas. El debido proceso requiere que los Estados respeten y garanticen los derechos humanos de los individuos asegurando que los procesos legales que regulan las injerencias en los derechos humanos estén detallados debidamente en la ley, se apliquen de manera coherente, y estén disponibles al público. El principio reconoce que "toda persona tiene derecho a una audiencia pública y justa dentro de un plazo razonable

por un tribunal independiente, competente e imparcial establecido por ley, salvo en casos de emergencia donde exista un riesgo inminente para la vida humana". En esos casos, debe buscarse una autorización retroactiva dentro de un lapso razonable y viable. La autorización con efecto retroactivo no puede estar justificada con la mera preocupación de riesgo de fuga o de destrucción de pruebas.

MÉXICO: El artículo 16 de la constitución establece que la interceptación de cualquier comunicación privada debe ser autorizada por una "autoridad judicial federal exclusivamente, bajo petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente. Para ello, la autoridad deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, civil, laboral, o administrativo, ni en el caso de las comunicaciones del detenido con su defensor".

La Suprema Corte de México (SCJN) también indicó, por ejemplo, que acceder y analizar los datos almacenados en un teléfono celular sin que medie una orden judicial es una injerencia en el derecho a la inviolabilidad de las comunicaciones privadas.[202] De la misma manera, la SCJN resolvió recientemente que el acceso a los metadatos de las comunicaciones almacenadas por las compañías de telecomunicaciones debe contar con una autorización judicial previa.[203] La SCJN consideró que la interceptación de un e-mail (de manera tal que vulnere el derecho a la inviolabilidad de las comunicaciones) se da en el momento en que se toma la contraseña de una cuenta sin orden judicial o sin el consentimiento del usuario, sin importar si se analiza el contenido de ese e-mail o no.[204]

Con respecto a los datos de ubicación, si bien la interpretación constitucional considera que los metadatos de las comunicaciones están protegidos de la misma manera que el contenido de las comunicaciones (en el sentido de que el acceso a ambos requiera autorización judicial), la Suprema Corte de Justicia indicó que no es necesario contar con una autorización judicial para el monitoreo de los datos de ubicación en tiempo real. Un ejemplo es la resolución de la SCJN con respecto a la acción de inconstitucionalidad 32/2012,[205] en la que la mayor parte de la Suprema Corte estimó que es constitucional permitir que la Procuraduría General (PGR) monitoree la geolocalización de teléfonos móviles en tiempo real, sin la necesidad de que media una orden judicial federal.

COLOMBIA:[206] La Corte Constitucional ha señalado que la regla general en el sistema

202 Corte Suprema. Sala de Primera Instancia. Contradicción de Tesis 194/2012.

203 Corte Suprema. Sala Segunda. Amparo en Revisión 964/2015.

204 Corte Suprema. Sala de Primera Instancia. Amparo en Revisión 1621/2010.

205 Corte Suprema. Sesión Plenaria. Acción de Inconstitucionalidad 32/2012.

206 Fragmento del reporte de Colombia, Juan Camilo Rivera y Katitza Rodriguez, "Vigilancia Estatal de las Comunicaciones y la Protección de los Derechos Fundamentales en Colombia",

jurídico colombiano es que las decisiones que restringen los derechos fundamentales de los investigados e imputados deben estar previstas por la ley y ser autorizadas por un juez (reserva judicial).[207] De manera excepcional, se confiere a la Fiscalía General de la Nación facultades que limitan los derechos de las personas, con la intención de permitir el recaudo de información relevante para los fines de un proceso penal, pero sujeta a un control de legalidad posterior a la actuación. Esta excepción opera solamente para los casos de registros, allanamiento, incautaciones e interceptaciones de comunicaciones.[208] La mencionada excepción debe ser interpretada de manera restrictiva, para evitar que se eluda la garantía de la autorización judicial previa para la afectación de los derechos. En virtud de esta regla, por ejemplo, la Corte Constitucional ha sostenido que actuaciones como la búsqueda selectiva de información confidencial de una persona indicada o sindicada en bases de datos no puede ser una de las actividades realizadas con orden de la Fiscalía General de la Nación sujeta a control judicial posterior.[209] Por lo tanto, la Corte ha exigido que, para proceder con dichas búsquedas, debe mediar autorización judicial previa.

Sin embargo, la Fiscalía General tiene permitido interceptar comunicaciones; capturar datos almacenados en dispositivos y mecanismos; y rastrear a los individuos, objetos, o lugares involucrados en una investigación penal sin contar con una autorización judicial previa, pero con el posterior control de legalidad correspondiente. El Código Procesal Penal establece los casos y procedimientos en los que la Fiscalía General puede hacer uso de este control de legalidad posterior. Indica que la interceptación de comunicaciones debe estar sujeta a control judicial dentro de las siguientes 36 horas, entre otros requisitos.[210]

Comisión Colombiana de Juristas, Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

207 Acción de inconstitucionalidad presentada por Pedro Pablo Camargo contra el segundo párrafo del artículo 2, el tercer párrafo del artículo 3 y la primera sección del artículo 5 del Acto Legislativo Nº 03 de 2002, "por el cual se reforma la Constitución Nacional", sentencia C-1092, Corte Constitucional, 19 de noviembre de 2003, disponible en: http://www.corteconstitucional.gov.co/relatoria/2003/C-1092-03.htm

208 Acción parcial de inconstitucionalidad presentada por Alejandro Decastro González contra los artículos 14, 244 y 246 de la Ley 906 de 2004 "por la cual se expide el Código de Procedimiento Penal", sentencia C-336, Corte Constitucional, 9 de mayo de 2007, http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

209 Acción parcial de inconstitucionalidad presentada por Alejandro Decastro González contra los artículos 14, 244 y 246 de la Ley 906 de 2004 "por la cual se expide el Código de Procedimiento Penal", sentencia C-336, Corte Constitucional, 9 de mayo de 2007, http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

210 Artículos 235 y 237 del Código Procesal Penal. Este lapso de 36 horas está compuesto por 12 horas para que la policía judicial informe al fiscal que se dio la orden de interceptación de las comunicaciones, más 24 horas que se le da al fiscal para que realice los controles judiciales ante un juez penal. Vea la acción de inconstitucionalidad de Gustavo Gallón et al. contra los artículos 14, 15 (parcial) y 16 de la Ley 1142 de 2007, "por medio de la cual se reforman parcialmente las Leyes 906 de 2004, 599 de 2000 y 600 de 2000 y se adoptan medidas para la prevención y represión de la actividad delictiva de especial impacto para la convivencia y seguridad ciudadana", sentencia C-131, Corte Constitucional, 24 de febrero de 2009 —en la

La legislación procesal penal también estipula que las "autoridades competentes" deben estar a cargo de los procedimientos técnicos para la interceptación de las comunicaciones y su procesamiento. A pesar de que la ley resulta muy general en relación con las autoridades encargadas de realizar los procedimientos, la Corte Constitucional la aprobó. La Corte argumentó que la ley sí especifica cuáles son las autoridades que dan la orden y realizan la interceptación —la Fiscalía General de la Nación— y le concede a esta el poder de decidir qué autoridades llevarán a cabo la interceptación y su procesamiento.

Además, si bien la ley no especifica quiénes son estas "autoridades competentes", estas se pueden determinar mediante una interpretación sistemática de las regulaciones concernientes al procedimiento técnico de la interceptación de las comunicaciones. Al interpretar el artículo 46 de la Ley 938 de 2004, la Corte estipula que la competencia mencionada recae sobre las autoridades de la policía judicial —actualmente, los que cumplen estas funciones son los Cuerpos Técnicos de la Policía Judicial y la Policía Nacional.[211]

La Fiscalía General también tiene el poder de ordenar la recuperación de información de registros de Internet u otras tecnologías similares del acusado durante una investigación penal, siempre y cuando medie una autorización judicial dentro de las 36 horas siguientes a la captura de dicha información, junto con otros requisitos.[212]

El artículo 17 de la Ley 1321 establece la diferencia entre la interceptación de las comunicaciones y el monitoreo del espectro electromagnético. La legislación colombiana prevé que las agencias de inteligencia no están facultadas para interceptar comunicaciones; solamente están autorizadas a monitorear el espectro y pueden solicitar datos almacenados a los PSI. En el contexto penal, existe un control judicial para las investigaciones penales que requieren interceptar comunicaciones, pero dicho control no aplica a las agencias de inteligencia, debido a que según la ley, las agencias de inteligencia únicamente están autorizadas a monitorear el espectro y no a interceptar las comunicaciones.

El artículo 29 de la Constitución de Colombia establece más salvaguardas relacionadas con el debido proceso, e indica que cualquier evidencia obtenida en violación del debido proceso "es nula".

---

que se realizó un estudio de constitucionalidad sobre el artículo 237 de la Ley 906 de 2004. http://www.corteconstitucional.gov.co/ RELATORIA/2009/C-131-09.htm

211 Acción parcial de inconstitucionalidad de Dagoberto José Lavalle contra el artículo 52 de la Ley 1453 de 2011 "por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad", sentencia C-594, Corte Constitucional, (2014). http://www.corteconstitucional.gov.co/RELATORIA/2014/C-594-14.htm

212 Artículos 236 y 237 del Código Procesal Penal.

ARGENTINA: En el contexto penal, se permite la interceptación de las comunicaciones solamente con una orden judicial.[213] La debe llevar a cabo la autoridad a cargo de la interceptación de las comunicaciones: la Dirección de Captación de Comunicaciones del Poder Judicial (DCCPJ), que funciona como una dependencia de la Corte Suprema.

Con respecto a la autorización judicial para acceder a los metadatos y a los datos de ubicación, no existe una regla clara, pero una resolución de la Corte Suprema estimó que se encuentran al mismo nivel que los "documentos privados", que se encuentran protegidos por el artículo 18 de la Constitución Nacional. Por lo tanto, aplican las mismas reglas (autorización judicial previa) para los metadatos y para el contenido de las comunicaciones personales.

En Argentina, la garantía constitucional que impide el acceso a los "documentos privados" no protege estrictamente el acceso a la información del suscriptor. El juez puede solicitar a un PSI o a una compañía de telecomunicaciones que brinden información sobre un suscriptor de manera directa, y el proveedor está obligado a cumplir con este pedido.

En el ámbito de la inteligencia y la contrainteligencia, la interceptación de las comunicaciones y el acceso al contenido de estas solo está permitido cuando medie una orden judicial, y es la DCCPJ la encargada de realizar estas acciones. Esto tiene su origen en las reglas que rigen las actividades de inteligencia y contrainteligencia, definidas por ley como inteligencia recopilada con propósitos de seguridad nacional, para la prevención de actividades llevadas a cabo por actores que plantean un riesgo para la seguridad estatal, y con el objetivo de investigar actividades delictivas graves.[214] Estas reglas aplican a la Agencia Federal de Inteligencia (AFI) desde diciembre de 2015. Sin embargo, debido a que la DCCPJ es la responsable de emitir la autorización judicial y reporta directamente a la Secretaría de Inteligencia, no se puede concluir que esta sea un mecanismo de control judicial independiente, ya que la Dirección está bajo la supervisión de un organismo de inteligencia dentro del Poder Ejecutivo.[215]

BRASIL: Si bien la legislación parece exigir supervisión judicial para todas y cada una de las interceptaciones de comunicaciones, los tribunales que interpretan estas leyes cambian el grado de supervisión judicial y el debido proceso dependiendo de qué vigile el Estado: el contenido de las comunicaciones o la información de los suscriptores. Esto se puede explicar

213 Los jueces se encargan de las investigaciones penales. El Nuevo Código Procesal Penal, actualmente suspendido, le dará esta facultad a los fiscales.

214 Ley de Inteligencia Nacional No. 25.520 de 2001, artículo 2.

215 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. (ADC) Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

en parte por la prohibición constitucional del anonimato en Brasil, que se ha usado injustamente para justificar el acceso a los datos del suscriptor como medio de identificación de delincuentes.

El acceso al contenido de las comunicaciones exige la observancia de las protecciones constitucionales y de los requisitos legales específicos, que deben estar asegurados mediante orden judicial. La ley 9.296 de 1996 exige a las autoridades obtener una orden judicial antes de realizar cualquier interceptación. El *Marco Civil da Internet* (Ley 12.965 de 2014) también requiere autorización judicial para acceder a la información del suscriptor, los metadatos, los datos de ubicación y el contenido de las comunicaciones. A pesar de esto, las autoridades de aplicación de la ley interpretaron que ambas leyes permiten el acceso a la información del suscriptor sin contar con una orden judicial para las "autoridades competentes". No obstante, estas "autoridades competentes" no están especificadas.

Algunos tribunales resolvieron que es necesario contar con autorización judicial previa con arreglo a la Ley 9.296 de acceso a los datos de ubicación. Otras leyes permiten específicamente la vigilancia sin autorización judicial previa. Las leyes 12.850 y 9.613/99 autorizan a la policía civil y a la Fiscalía para obtener la información del suscriptor directamente de las compañías telefónicas sin contar con una orden.

No quedan claros los requisitos para acceder a los registros de llamadas. Si bien estos registros están protegidos por la Constitución y pueden, por lo tanto, divulgarse solamente mediante orden judicial, las interpretaciones abusivas de la Ley 12.850 permitieron la realización de solicitudes directas por parte de la aplicación de la ley para acceder a ellos.

PERÚ: El párrafo 10 del artículo 2 de la Constitución estipula que cualquier comunicación, telecomunicación, o correspondencia privada se se puede abrir, incautar, interceptar o intervenir por una autoridad unicamente con una orden emitida por un juez, y con todas las garantías provistas por ley. El marco legal peruano también deja en claro que solo un juez puede autorizar a un fiscal para escuchar y controlar las comunicaciones de un acusado sometido a investigación preliminar o judicial por un delito particular de la lista de ofensas.[216]

Lamentablemente, el Decreto Legislativo 1182[217] no incorpora el requisito de autorización judicial previa. En cambio, le concede a la policía acceso ilimitado, sin orden judicial y en tiempo real a los datos de ubicación del usuario y a la información del dispositivo en los

216 Vea la Ley 27.697 y los detalles en los Códigos Procesales Penales, y también el Protocolo de Actuación Conjunta de Intervención o Grabación de Registros de Comunicaciones Telefónicas u otras Formas de Comunicación, aprobada por Resolución Ministerial No. 0243-2014-JUS.

217 República del Perú. Decreto Legislativo No. 1182. http://www.elperuano.com.pe/NormasElperuano/2015/07/27/1268121-1.html

casos de flagrante delito.[218] El juez no revisará la observancia de estos requisitos hasta 72 horas después de que la policía haya accedido a los datos.

La mejor práctica es exigir que la autoridad judicial revise la legalidad de las actividades de vigilancia. En Perú, por ejemplo, las leyes de inteligencia exigen autorización judicial para implementar cualquier medida de vigilancia de las comunicaciones. En algunos casos excepcionales, la autorización judicial puede concederse después de llevadas a cabo las medidas. Así, el Decreto Legislativo 1141 de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional (SINA) y de la Dirección Nacional de Inteligencia (DINI) exige autorización de alguno de los dos jueces ad hoc del Poder Judicial (nombrados específicamente para esta tarea por la Suprema Corte) para llevar a cabo la vigilancia. No se aprobará la medida a menos que el Director de Inteligencia Nacional demuestre que la vigilancia es estrictamente indispensable para lograr los propósitos de las actividades de inteligencia.

Cuando existan amenazas para la seguridad nacional, y durante estados de emergencia, el Decreto Legislativo 1141 permite al Director Nacional de Inteligencia autorizar la ejecución de un procedimiento especial para la obtención de información bajo la condición de que la solicitud se formalice de manera inmediata ante un juez ad hoc quien, dentro de las siguientes veinticuatro horas, pueda validar u ordenar el cese del procedimiento. El Decreto también estipula que cuando un juez ordene la cesación del procedimiento especial, las autoridades pueden apelar esa decisión.

CHILE: El artículo 9 del Código Procesal Penal, titulado "Autorización judicial previa", indica que "toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa".

El artículo 222 del Código Procesal Penal aplica esta disposición a la interceptación telefónica y de telecomunicaciones. Estipula que un juez puede ordenar la interceptación cuando existan sospechas fundadas, basadas en hechos específicos, que sugieran que una persona ha cometido o está preparando un crimen. La ley limita los crímenes que pueden ser investigados de esta manera a aquellos que tendrían una pena de al menos cinco años y un día de privación de la libertad.

En el reporte sobre Chile, individualizamos un caso particular en que se usaron estos poderes en violación de este Principio:[219]

218 La ley peruana habla del flagrante delicto para referirse a un crimen en proceso de comisión, cometido recientemente o hasta 24 horas después de ser cometido.

219 Juan Carlos Lara y Valentina Hernández, "Vigilancia Estatal de las Comunicaciones y la Protección de los Derechos Fundamentales en Chile", Electronic Frontier Foundation & Derechos Digitales, (2016). https://necessaryandproportionate.org/country-reports/chile

[E]n abril de 2012 fue formalizada la investigación contra el exjefe de la Dirección de Inteligencia de Carabineros (Dipolcar), el mayor Gonzalo Alveal Antonucci, por supuestamente interceptar ilegalmente el celular de un efectivo policial y usar esas escuchas para obligar su alejamiento de la institución.[220]

Según la investigación, entre los meses de mayo y julio del año 2010, el entonces jefe de asuntos internos de la Dipolcar habría ordenado la interceptación telefónica de dos números celulares de funcionarios de la misma institución, sin mediar orden judicial y en el contexto de una investigación policial. Según lo entendió el Ministerio Público, esa información era utilizada para fines ajenos a la investigación en curso, por lo que el mayor Alveal Antonucci fue formalizado por los delitos de obstrucción a la investigación y grabación de comunicaciones privadas sin autorización judicial. La investigación llegó a término sin sentencia.[221]

En el contexto de inteligencia, la legislación chilena exige que las autoridades de inteligencia obtengan una orden judicial para realizar procedimientos para la obtención de información, usando uno de estos dos procedimientos:

El primero permite a la Agencia Nacional de Inteligencia solicitar información a distintas entidades estatales o recopilarla mediante información de acceso público. Por ejemplo, de acuerdo con el artículo 8 de la Ley 19.974, la Agencia Nacional de Inteligencia puede solicitar información a las autoridades militares y de aplicación de la ley y a autoridades de la seguridad pública (los Carabineros de Chile y la Policía de Investigaciones de Chile). También puede solicitar información a las diferentes agencias que pertenecen a la Administración del Estado y a las compañías e instituciones que dependen de las contribuciones del Estado.

Si, después de recibir la información de las agencias del estado, la Agencia de Inteligencia aún requiera información, se realiza independientemente un segundo procedimiento para la obtención de interceptaciones telefónicas, informáticas y de radiodifusión; la interceptación de sistemas informáticos y redes; escuchas telefónicas y grabaciones electrónicas, y; la interceptación de cualquier otro sistema tecnológico de transmisión, almacenamiento o procesamiento de comunicaciones electrónicas.

Se requiere autorización judicial para realizar estos procedimientos especiales, y solamente los directores o jefes de las agencias de inteligencia pueden presentar estas solicitudes. La

220 La Segunda, "Golpe a la inteligencia policial: Fiscalía formalizará a ex oficial por escuchas ilegales". Urzúa, M y Candia, V, 16 de marzo de 2013.

221 Juan Carlos Lara y Valentina Hernández, "Vigilancia Estatal de las Comunicaciones y la Protección de los Derechos Fundamentales en Chile", Electronic Frontier Foundation & Derechos Digitales, (2016). https://necessaryandproportionate.org/country-reports/chile

autorización para el uso de los procedimientos especiales es emitida directamente por el Ministro de la Corte de Apelaciones del territorio en el que se lleve a cabo o se inicie el procedimiento, o por el juez institucional correspondiente.

El Código Procesal Penal establece más salvaguardas relacionadas con el debido proceso, e indica que cualquier evidencia que se haya obtenido en violación de la ley será omitida en el proceso legal.

EL SALVADOR: El artículo 176 del Código Procesal Penal (CPP) contempla la libertad de presentar cualquier hecho o circunstancia de un caso como elemento probatorio en un proceso penal, siempre que esta evidencia se haya obtenido respetando todas las garantías constitucionales y legales. El artículo primero de la Ley de Intervenciones de las Comunicaciones deja asentada la naturaleza excepcional de la vigilancia de las comunicaciones, y la necesidad de que medie una orden al momento de tomar dichas medidas. También asegura la confidencialidad de toda la información privada que haya sido obtenida mediante la interceptación de las comunicaciones, pero no tiene relación con la investigación ni los procesos penales. La información que haya sido obtenida de manera ilegal, pasando por alto el debido proceso, quedará sin valor probatorio.

GUATEMALA: Este país exige que medie una orden para la interceptación de las comunicaciones. Además, se exige a los jueces que supervisen la interceptación de las comunicaciones para asegurar que operen de conformidad con la ley.[222]

222 Capítulo de Guatemala. Jorge Jiménez Barillas Hedme Sierra-Castro. Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos? un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.). -- 1a. ed.-- San José, C.R.: Fundación Acceso, 2015. pdf; p. 151

7.
Supervisión Pública

Los estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones.

Las democracias están basadas en la repartición de los poderes. El fin de dividir los poderes del estado en las ramas judicial, legislativa y ejecutiva es crear un equilibrio de poderes. Cada poder posee mecanismos establecidos para supervisarse a sí mismo y a los restantes, para prevenir el monopolio del poder y abusos.[223]

El control interno del poder ejecutivo generalmente consiste en una comisión dentro del mismo sistema de inteligencia nacional. El control externo se encuentra usualmente fuera del sistema de inteligencia, pero dentro del poder ejecutivo —a menudo este control se asigna al Ministerio del Interior y Defensa.

En lo que respecta a la rama legislativa, el tipo de supervisión establecida depende de si el Congreso o el Parlamento es un organismo unicameral o bicameral. Por ejemplo, si existe un parlamento bicameral, este puede tener una comisión de supervisión por cada órgano del congreso o solamente una comisión que tenga miembros de ambas cámaras.

Finalmente, el control sobre el poder judicial se implementa frecuentemente con la solicitud de una autorización judicial para llevar a cabo la vigilancia durante las investigaciones penales o de inteligencia nacional, aunque estos sistemas rara vez brindan la supervisión pública que requiere el principio. En algunos sistemas legales, los grandes jurados civiles y públicos llevan a cabo funciones de supervisión y auditoría en varios tipos de operaciones gubernamentales y podrían ser, sin dudas, implementados para la revisión de programas de vigilancia. En otros casos, el poder judicial nombra a un Perito Especial para que supervise y monitoree un programa, en particular cuando el programa necesita sufrir una reforma significativa. Estos peritos especiales se aseguran de que el programa opere de conformidad con la ley y pueden sugerir cambios en los programas de vigilancia. En algunos casos particulares, puede haber un órgano judicial encargado de supervisar el sistema de inteligencia completo, pero este tipo de control no existe en América Latina.

223 José Manuel Ugarte. La conceptualización de los diferentes tipos de controles de supervisión en el marco de la inteligencia y contrainteligencia tiene su base en: José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. (ADC) Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

Desgraciadamente, no existe la tradición de supervisión pública en las actividades de inteligencia en América Latina. La mayoría de las agencias de inteligencia latinoamericanas se formaron en tiempos en que la división de poderes no existía —es decir, bajo regímenes militares en los que las operaciones estaban incrustadas en el poder ejecutivo.[224] Debido a que estas agencias de inteligencia formaban parte de dictaduras militares, la mayoría de los gobiernos hizo una transición hacia la democracia mediante un proceso de negociación con la junta militar, y por eso se crearon sin los controles adecuados y sin mecanismos de supervisión pública.

El bajo rendimiento de los mecanismos de control existentes tiene, entonces, relación con la poca o nula cultura democrática de las organizaciones de inteligencia. Los organismos de inteligencia en América Latina se formaron en un momento en que los regímenes democráticos eran débiles, autoritarios o inexistentes. Por lo tanto, los mecanismos de control se colocaron sobre la base de una cultura heredada no democrática.

Más aún, la naturaleza reforzada del presidencialismo latinoamericano también explica por qué los mecanismos de supervisión tienen un pésimo rendimiento.[225] En la región, los presidentes son formalmente más poderosos que, por ejemplo, sus pares de Estados Unidos (pueden declarar emergencias, pueden presentar una legislación en el Congreso).

Por otro lado, se ha argumentado que la dinámica política en la región por lo general crea una situación en que el Congreso delega su poder en el presidente, ya sea de iure o de facto, al menos en los primeros momentos de una presidencia.[226] Si estos análisis son correctos, podrían explicar por qué los mecanismos de supervisión legislativa no funcionan. Las agencias de inteligencia en América Latina han sido herramientas poderosas en la política presidencial, especialmente utilizados para espiar a los grupos disidentes, políticos de oposición y periodistas independientes.[227]

Estos abusos han sido ampliamente documentados: desde los escándalos involucrando al peruano Vladimiro Montesinos, ex director del Servicio de Inteligencia (SIN) en la década de 1990 a las reveladoras escuchas telefónicas del servicio de inteligencia (DAS) de la década de 2000 en Colombia, a la convulsión más reciente relacionado con los servicios de

224 José Manuel Ugarte. El control público de la actividad de inteligencia en América Latina. Ediciones CICCUS, Buenos Aires, 2012.

225 Mainwaring, Scott. "Presidentialism in Latin America." Latin American Research Review 25, no. 1 (1990): 157–179, 160.

226 O'Donnell, Guillermo A., ed. *Counterpoints: Selected Essays on Authoritarianism and Democratization*. First Edition edition. Notre Dame, Ind: University of Notre Dame Press, 2003.

227 *See* Ramiro Álvarez Ugarte and Emiliano Villa. El (des)control de los organismos de inteligencia en la Argentina. Asociación por los Derechos Civiles (ADC). January 2015. Available at: http://www.adc.org.ar/wp-content/uploads/2015/01/2015-01-23-Informe-Final-Inteligencia.pdf

inteligencia en la Argentina. El uso de los servicios de inteligencia para apoyar las políticas y los deseos presidenciales es posiblemente la variable que explica con más fuerza por qué los mecanismos de supervisión no funcionan. La naturaleza delegativa de la política presidencial explica, por otra parte, porque los mecanismos de supervisión legislativa por lo general se acercan a su tarea con un *laissez faire* (dejar hacer), que es incompatible con las exigencias de las sociedades democráticas modernas.

Estas debilidades institucionales sólo pueden superarse si una sociedad civil fuerte demanda transparencia y rendición de cuentas de los servicios de inteligencia. Estos esfuerzos son generalmente superados por el secreto que rodea tanto a las actividades como a las organizaciones de inteligencia. Sin embargo, los avances producidos en la última década en leyes de acceso a la información, en toda la región deben ofrecer una oportunidad para perforar a través de estos obstáculos con el fin de fortalecer la capacidad de los ciudadanos de supervisar esa parte del estado que permanece en la oscuridad.

Además de mejorar el diseño institucional para la supervisión y el control de las actividades de inteligencia, la región debería comprometerse a implementar mecanismos de supervisión pública y desarrollar una sociedad civil fuerte que trabaje en este tema.

EL SALVADOR: El Ministerio Público (compuesto por el Fiscal General y la Procuraduría General) es el encargado de supervisar la interceptación de las comunicaciones.[228] Ambas agencias gubernamentales están autorizadas para auditar a la agencia responsable de interceptar comunicaciones, aunque sus resoluciones no son jurídicamente vinculantes.[229] Los artículos 23 y 26 de la Ley para la Intervención de las Telecomunicaciones prevén que el Fiscal para la Defensa de Derechos Humanos y el Fiscal General poseen la facultad jurídica de redactar el "Protocolo de Funcionamiento del Centro de Intervención", por el cual deben realizar auditorías periódicas. También tienen el derecho de llevar a cabo auditorías anuales de las actividades del Centro de Intervención y presentar informes relevantes a la Comisión de Legislación y Puntos Constitucionales de la Asamblea Legislativa.

La ley habilita al fiscal a realizar auditorías específicas relacionadas con la violación del derecho a la privacidad y a la secrecía de las comunicaciones cuando así lo crea necesario. Estas auditorías específicas se incorporan en un anexo al informe general dirigido a la

228 Capítulo de El Salvador. Marlon Hernández Anzora. Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos? un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.) p. 90-91

229 Capítulo de El Salvador. Marlon Hernández Anzora, Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos? un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.) p. 90-91

Comisión Legislativa. El artículo 31 de la misma ley estipula que el funcionamiento y la seguridad del Centro de Intervención estarán descriptos en un reglamento elaborado por el fiscal. Esto crea un conflicto de intereses para los fiscales, debido a que es la responsabilidad del fiscal desarrollar los reglamentos que él mismo aplicará en todos casos penales, en los que es el demandante.

ARGENTINA: La Comisión Bicameral Permanente de Fiscalización de los Organismos y Actividades de Inteligencia es el mecanismo de control legislativo de este país. Esta Comisión se creó en 2001, con la promulgación de la Ley Nacional de Inteligencia 25.520, y comenzó a funcionar en 2004.[230] Según la Ley Nacional de Inteligencia, las responsabilidades de la Comisión comprenden supervisar las agencias del Sistema Nacional de Inteligencia, monitorear su funcionamiento para asegurar que cumpla con las reglamentaciones legales y constitucionales, y controlar las actividades de inteligencia. La ley concede a la Comisión "amplias facultades para controlar e investigar de oficio". Por ejemplo, la Comisión puede intervenir en cualquier legislación que afecte a las actividades de inteligencia. También se le exige la redacción de un informe anual confidencial sobre la efectividad del Sistema Nacional de Inteligencia para ser entregado al Congreso Nacional.[231]

Lamentablemente, la efectividad general de la Comisión se ve afectada por distintos factores.

En primer lugar, el poder ejecutivo básicamente controla la información que ve la Comisión. La ley impone una restricción general sobre la información relativa a las actividades de inteligencia y contrainteligencia: "El acceso a dicha información será autorizado en cada caso por el Presidente de la Nación o el funcionario en quien se delegue expresamente tal facultad".[232] Entonces, la Comisión necesita la autorización de la Secretaría de Inteligencia (parte del sistema de inteligencia en el poder ejecutivo) para tener acceso a esta información.[233]

En segundo lugar, la Comisión opera, mayoritariamente, en secreto. Organizaciones de la

---

230 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. (ADC) Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

231 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. (ADC) Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

232 República Argentina, Ley No. 25.520 de Inteligencia Nacional, Boletín Oficial del 6 de diciembre del 2011, artículo 16.

233 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. (ADC) Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

sociedad civil —Asociación por los Derechos Civiles (ADC) y el Instituto Latinoamericano de Seguridad y Democracia (ILSED)— afirman que, a pesar de haber solicitado información sobre las actividades operativas de la Comisión Bicameral, no recibieron respuesta a dichas peticiones.[234]

Por otro lado, como hemos mencionado anteriormente, el informe obligatorio de la Comisión tiene carácter reservado, y no es de acceso público;[235] sin embargo, la ADC y el ILSED descubrieron que se les entregó una copia del informe a los diputados argentinos.[236]

En un informe publicado en el 2015 y en medio del escándalo por la muerte del fiscal Alberto Nisman, ADC concluyó que la Comisión Bicameral opera en un secreto tal que hace imposible evaluar si está funcionando correctamente o si funciona en absoluto. Los testimonios recogidos en el curso de dicha investigación sugieren que la última sospecha es la conclusión correcta.[237] Una coalición de organizaciones de la sociedad civil trabajando por la transparencia del sector inteligencia ha argumentado durante el 2016 que las nuevas decisiones del gobierno sobre la materia no sólo no resuelven los viejos problemas que enfrenta la comunidad de inteligencia en la Argentina, más bien los empeoran nombrando, por un lado, funcionarios partidistas sin experiencia, y por otro, gente con estrechos vínculos con miembros de la comunidad sospechosos de llevar a cabo inteligencia ilegal contra figuras públicas, contrabando ilegal de bienes y trafico de drogas.[238]

CHILE: Dentro del Poder Ejecutivo, las agencias de inteligencia se unificaron progresivamente desde 2004 bajo la Agencia Nacional de Inteligencia (ANI). La ANI posee controles de supervisión e informa directamente al Ministerio del Interior. También existe una supervisión parlamentaria llevada a cabo por la Cámara de Diputados, la cual es muy

234 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles., ADC. p. 14 https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

235 El artículo 13.9 y el 33.3 de la Ley No. 25.520 exigen a la Comisión emitir un informe nacional anual para el Congreso sobre todas las actividades de inteligencia que supervisa.

236 José Ramiro Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles, ADC. https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

237 Ramiro Álvarez Ugarte and Emiliano Villa. Who is Watching the Watchers? Privacy International. Asociacion por los Derechos Civiles, ADC. https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

238 ICCSI. AFI: las declaraciones de Arribas y Majdalani que confirman que el Senado no debe brindarles el acuerdo (2016). http://www.iccsi.com.ar/afi-las-declaraciones-de-arribas-y-majdalani-que-confirman-que-el-senado-no-debe-brindarles-el-acuerdo. ICCSI, Acuerdo para no innovar (2016). http://www.iccsi.com.ar/agencia-federal-de-inteligencia-acuerdo-para-no-innovar

limitada, debido a que la cámara no posee facultades de investigación.[239] El artículo 37 de la Ley 19.974 prescribe que el sistema de inteligencia informará sobre sus actividades a la comisión del congreso. Ya que el Director de la ANI elabora el informe anual sobre las operaciones de inteligencia y su desempeño, el informe no es independiente y sus hallazgos no son públicamente verificables porque no es de acceso público y las operaciones descritas en él se llevan a cabo dentro de comisiones secretas.

El artículo 36 estipula que la Contraloría General de la República evaluará la legalidad de los decretos expedidos por la ANI. Las decisiones de la Contraloría General sobre la legalidad se toman mediante un proceso constitucional documentado (llamado toma de la razón) y se clasifican según la misma ley. Si bien Chile impone más responsabilidades de supervisión a su Contraloría General y al Parlamento, estos procesos no son públicos.

PERÚ: En el 2000, el expresidente Fujimori desmanteló el Sistema de Inteligencia Nacional (SIN), a raíz de que un escándalo de corrupción dentro de la agencia fue hecho público.[240] En 2006, la Ley 28.664 creó el Sistema de Inteligencia Nacional (SINA) y la Dirección Nacional de Inteligencia (DINI), que se especializan en inteligencia nacional no militar y se reportan directamente con el Presidente.[241]

La Comisión de Inteligencia del Congreso de Perú funciona como control legislativo y supervisa todas las actividades del SINA. Revisa los planes de inteligencia y todos los archivos presentados a los jueces a cargo de las solicitudes de interceptación de las comunicaciones. La Comisión también recibe un informe anual directamente del Director de Inteligencia. A diferencia de otros países, la Comisión puede investigar de oficio, pero debe hacerlo bajo la dirección de otra agencia de inteligencia: la DINI.[242] Por lo tanto, no queda definido el alcance de la investigación.

A pesar de estos controles, Perú no ha tenido éxito en la prevención de abusos por parte de las agencias de inteligencia, aunque sí ha existido cierta rendición de cuentas de manera pública. Las investigaciones periodísticas resultaron en quejas con respecto a la participación

239 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. (ADC) Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

240 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. ADC. https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

241 José Manuel Ugarte. El control público de la actividad de inteligencia en América Latina. Ediciones CICCUS, Buenos Aires, 2012.

242 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

de la DINI en la vigilancia ilegal de políticos, empresarios, y periodistas. Consecuentemente, en febrero de 2015, la Presidenta del Consejo de Ministros anunció la decisión de disolver la DINI y reorganizar la estructura nacional de inteligencia desde cero. Un mes más tarde, estas revelaciones provocaron una moción de censura exitosa de todo el gabinete de ministros presidido por Ana Jara, la cual resultó ser la primera censura en el país en más de 52 años.[243] Inmediatamente, se sometió al sistema de inteligencia a una reestructuración.[244]

COLOMBIA: La ley de inteligencia colombiana (No. 1621 de 2013) establece un control interno y externo sobre las actividades de vigilancia.[245] Los inspectores dentro de las agencias de inteligencia deben presentar un informe anual al Ministerio de Defensa que describa las actividades de inteligencia llevadas a cabo dentro de su marco legal y de conformidad con la Constitución.[246] La Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia debería recibir una copia de este informe.[247]

Además, Colombia cuenta con una Junta de Inteligencia Conjunta, compuesta por los directores de cada una de las fuerzas militares de Colombia y el Ministerio de Defensa.[248] La Junta está a cargo de la supervisión de todas las agencias de inteligencia con arreglo al Plan de Inteligencia,[249] y debe presentar un informe anual ante la Comisión Legal. Ambos informes contienen información clasificada y no son de acceso público.[250]

El Poder Legislativo se encarga del control externo, especialmente la Comisión Legal de

---

243 El Comercio, "Ana Jara fue censurada por el Congreso por rastreos de la DINI". 31 de marzo de 2015. http://elcomercio.pe/politica/congreso/ana-jara-congreso-debatira-pedido-censura-caso-dini-noticia-1801055

244 El Comercio, "Gobierno cerrará la DINI por 180 días para su reestructuración", 9 de febrero de 2015. http://elcomercio.pe/politica/congreso/ana-jara-congreso-debatira-pedido-censura-caso-dini-noticia-1801055

245 República de Colombia, Ley No. 1521 de 2013. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

246 República de Colombia, Ley No. 1521 de 2013. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf Artículo 18.

247 República de Colombia, Ley No. 1521 de 2013. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf. Artículo 18.

248 República de Colombia, Ley No. 1521 de 2013. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf. Artículo 12.

249 República de Colombia, Ley No. 1521 de 2013. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf. Artículo 12.

250 República de Colombia, Ley No. 1521 de 2013. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf. Artículos 18 y 13 (h).

Seguimiento a las Actividades de Inteligencia y Contrainteligencia. Esta comisión tiene tres funciones principales: llevar a cabo la supervisión y controles políticos, verificar que el uso de los recursos sea eficiente, y comprobar la legalidad de las prácticas de las agencias de inteligencia.

Los poderes conferidos a la Comisión Legal tienen el objetivo de controlar el desempeño de los mecanismos de supervisión de las actividades de inteligencia. El artículo 22 de la Ley 1621 de 2013 indica que la Comisión Legal deberá ser capaz de reunirse con la Junta de Inteligencia Conjunta, tomar conocimiento de los informes anuales elaborados por los inspectores, solicitar información adicional a ellos y a las oficinas de control interno, convocar a los jefes y directores de las agencias de inteligencia, y familiarizarse con los objetivos de la inteligencia nacional esbozados en el Plan Nacional de Inteligencia. Sin embargo, para verificar la legalidad de las actividades de las agencias de inteligencia y contrainteligencia, la Comisión Legal se ve limitada porque solamente puede intervenir en la información que las agencias le entreguen. Esto genera problemas, ya que muchas de las actividades de estas agencias no se informan o son de carácter clasificado.

Por último, la ley de inteligencia colombiana tiene dos salvaguardas adicionales. El artículo 18 protege a los informantes. Dicta que todos los miembros de las agencias de inteligencia y contrainteligencia deben informar sobre irregularidades relativas a las actividades realizadas dentro de sus agencias al Inspector de cada una o al jefe de la Oficina de Control Interno. Se protegerá la identidad del informante en todos los casos. Además, el artículo 23 exige que se realice una evaluación de la credibilidad de la Comisión misma, al menos una vez al año.

Según la Ley 1321 de 2013, la Comisión Legal tiene ocho miembros, cuatro senadores y cuatro miembros de la Cámara de Representantes.[251] La Comisión Legal actualmente no está operando.

BRASIL: Brasil brinda otro ejemplo de los límites impuestos sobre los mecanismos de supervisión política, lo que impide la transparencia de las actividades de las agencias de inteligencia y contrainteligencia.

El Poder Ejecutivo posee mecanismos de control internos y externos. El Director General de la ABIN posee el control interno de la supervisión, mientras que la Cámara de Relaciones Exteriores y Defensa Nacional tiene el control externo. Según los analistas de políticas de inteligencia, no queda claro si la última desempeñará sus funciones de manera permanente.[252]

---

251 Página web del Congreso Visible. Universidad de Los Andes. Disponible en: http://www.congresovisible.org/comisiones/39/

252 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. (ADC) Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the

En el contexto legislativo, existe una Comisión Mixta en el Congreso Nacional que está a cargo de supervisar a dichas agencias. No obstante, la información sobre el funcionamiento de esta Comisión es casi inexistente, a excepción de que desde su creación en el 2000, ha mantenido dos o tres reuniones por año.[253] Además, hay muy poca información sobre el Sistema Brasilero de Inteligencia (SISBIN).

No existen entidades de supervisión en la rama judicial; sin embargo, las solicitudes para la interceptación de las comunicaciones o el acceso a los datos sí precisan una autorización judicial (*Marco Civil de Internet*, artículo 10.1).

URUGUAY: Uruguay carece de mecanismos de supervisión externos. Se caracteriza por poseer un sistema de inteligencia descentralizado y fragmentado, lo que dificulta la supervisión coordinada y centralizada.[254] En 2010, Uruguay comenzó un proceso de reestructuración del sistema de inteligencia para centralizar a todas las agencias bajo el Sistema de Inteligencia Nacional. En 2014, el proyecto de ley fue rechazado y actualmente se ha presentado de nuevo ante el Parlamento uruguayo.[255]

HONDURAS: Honduras no cuenta con un organismo de supervisión independiente que controle las actividades de inteligencia.[256]

%20Watchers_0.pdf

253 José Manuel Ugarte. ¿Quién vigila a quienes vigilan? Privacy International. Asociación por los Derechos Civiles. (ADC) Disponible en: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

254 Samanta Curti. "Reformas de los Sistemas de Inteligencia en América del Sur". http://www.kas.de/wf/doc/17940-1442-1-30.pdf

255 El País. Reflotan Proyecto de Ley de Inteligencia. http://www.elpais.com.uy/informacion/reflotan-proyecto-ley-inteligencia.html

256 Capítulo de Honduras. Edy Tábora Gonzales. Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos? un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.).p. 229

8.
Integridad de las comunicaciones y sistemas

Los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de vigilancia de las comunicaciones del estado. Las personas tienen el derecho a expresarse anónimamente, por lo que los Estados deben abstenerse a obligar la identificación de los usuarios.

El Principio de Integridad de las Comunicaciones y Sistemas busca la protección contra las obligaciones tecnológicas que ponen en riesgo la infraestructura del proveedor de servicios. También protege la libertad de resguardar las comunicaciones propias mediante el uso de la tecnología de cifrado y la habilidad de comunicarse de manera anónima.[257]

El derecho a usar el cifrado

El cifrado protege la seguridad de las comunicaciones de los individuos. También protege la libertad de expresión impidiendo que los sistemas de censura técnica y automatizada bloqueen el acceso a un contenido determinado (o incluso a palabras clave determinadas). Promueve la expresión indirectamente, brindando a los usuarios la confianza en que sus comunicaciones o sus historiales de búsqueda están protegidos por medios técnicos.

Sin el cifrado, las comunicaciones en línea son muy fáciles de interceptar.[258] Los intermediarios de Internet que almacenan y procesan nuestras comunicaciones a menudo

257 Este fragmento pertenece a un escrito de nuestra elaboración. Vea Katitza Rodriguez, EFF. "Observaciones presentadas ante el Relator Especial de la ONU para la promoción y protección del derecho a la libertad de opinión y expresión" [Comments Submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression], 2015, https://www.eff.org/document/eff-comments-submitted-united-nations-special-rapporteur-promotion-and-protection-right

258 Vea, por ejemplo, Firesheep (2010). Recuperado el 6 de febrero de 2015, de la página http://codebutler.com/firesheep. Vea también John P. Mello Jr. , Ofrecen herramienta gratis para combatir a los hackers de Firesheep [Free Tool Offered To Combat Firesheep Hackers], PCWorld, Recuperado el 6 de febrero de 2015, de la página http://www.pcworld.com/article/211531/free_tool_offered_to_combat_firesheep_hackers.htm. Seth Schoen, Richard Esguerra (2010). El mensaje de Firesheep: "Sitios web maaaalos, ¡implementen HTTPS en todo el sitio ahora! [The Message of Firesheep: "Baaaad Websites, Implement Sitewide HTTPS Now!], EFF. Recuperado el 6 de febrero de 2015, de la página http://www.eff.org/deeplinks/2010/10/message-firesheep-baaaad-websites-implement. EFF, Herramienta ofrece nueva protección contra "Firesheep" [Tool Offers New Protection Against 'Firesheep'], 23 de noviembre de 2010. Recuperado el 6 de febrero de 2015, de la página http://www.eff.org/press/archives/2010/11/23

tienen la posibilidad de poseer y leer todas nuestras comunicaciones no cifradas que pasen por sus redes.[259] Los proveedores de servicios deberían ser capaces de diseñar sistemas que garanticen el cifrado de extremo a extremo: es decir, sistemas que aseguren que un mensaje puede ser leído únicamente por el receptor deseado.

A pesar de que el cifrado cumple una función central en todos los aspectos de la seguridad informática, los gobiernos generalmente desaprueban los intentos de hacer su uso más fácil y convenientemente accesible al público. Algunos Estados han intentado usar medidas legales para limitar el acceso del público a las herramientas de cifrado o para forzar a los productores y desarrolladores de *software* a brindar concesiones para el debilitamiento de la seguridad.[260] En casos sobresalientes, como en negociaciones a puertas cerradas, los gobiernos presionaron directamente a fabricantes individuales, amenazándolos con prohibir o bloquear sus productos y servicios. Desde 2010 hasta 2013, por ejemplo, el productor canadiense de teléfonos móviles BlackBerry participó en confrontaciones públicas con (por lo menos) los gobiernos de Arabia Saudita, los Emiratos Árabes Unidos, y la India, quienes objetaban el resistente uso del cifrado de los BlackBerry en Canadá, y sugerían que los productos BlackBerry debían estar prohibidos en sus territorios.[261] El fabricante accedió a brindar una solución que le confiera a los gobiernos el acceso para espiar a usuarios no empresariales.[262]

Hay quienes sostienen que no debería existir la "tecnología impenetrable". Esta exigencia equivale a una obligación tecnológica e insta a un marco regulatorio draconiano. Esto tiene consecuencias funestas sobre la innovación y la comunidad de código abierto en su totalidad. Algunos desarrolladores de código abierto ya se han pronunciado en contra de construir puertas traseras en los *softwares*.[263] Además, cualquier obligación adicional impuesta a los proveedores de servicios exigirá que estos inviertan una cantidad de dinero importante para hacer que sus tecnologías cumplan con las nuevas reglas, y estos gastos seguro se verán reflejados en el precio que paguen sus clientes.

---

259 Electronic Frontier Foundation, Resumen animado: Cuánto puede ayudar el cifrado a evitar la vigilancia en línea [Animated Overview: How Strong Encryption Can Help Avoid Online Surveillance], Surveillance Self-Defense, https://ssd.eff.org/en/module/animated-overview-how-strong-encryption-can-help-avoid-online-surveillance

260 Vea Bert-Jap Koops (2013), Estudio de la legislación sobre el cifrado [Crypto Law Survey]. Recuperado el 9 de febrero de 2015, de la página http://cryptolaw.org/ (enumera todos los controles conocidos de uso doméstico, exportación e importación sobre el cifrado).

261 Vea, por ejemplo, BBC News (2010), Dos Estados del Golfo prohibirán funciones del BlackBerry. Recuperado el 9 de febrero de 2015, de la página http://www.bbc.com/news/world-middle-east-10830485

262 Vea Wired News (2013), BlackBerry le concede al gobierno hindú la habilidad de interceptar mensajes [BlackBerry gives Indian government ability to intercept messages], recuperado el 9 de febrero de 2015, de la página http://www.wired.co.uk/news/archive/2013-07/11/blackberry-india

263 Zooko O'Whielacronx (2010), Comunicado sobre puertas traseras [Statement on Backdoors]. Recuperado el 6 de febrero de 2015, de la página http://tahoe-lafs.org/pipermail/tahoe-dev/2010-October/005353.html

Obligaciones tecnológicas

Las leyes que exigen a los proveedores de telecomunicaciones garantizar que las agencias de aplicación de la ley puedan tener acceso a sus registros, ya sea caso por caso o mediante la construcción de un punto de acceso permanente para el gobierno, puede ir en contra del Principio de Integridad de las Comunicaciones y Sistemas. Esta "vigilancia por diseño" es capaz de impedir la innovación en materia de privacidad ya que restringe la cantidad de opciones disponibles a aquellos que desarrollan servicios de Internet y servicios móviles.

La implementación de requisitos de capacidad técnica simplifica y automatiza las escuchas telefónicas y otros procesos de interceptación de comunicaciones, haciendo que la interceptación sea menos costosa, más rápida, y más conveniente. Dicha simplificación minimiza la participación y supervisión humana en el proceso, lo que puede reducir la habilidad del proveedor de impugnar o sacar a la luz escuchas ilegales y otros abusos. El equipo de escuchas también ha sido hackeado, activado de manera remota, y usado encubiertamente para realizar interceptaciones ilícitas con propósitos de espionaje. Las obligaciones técnicas son capaces de impedir que los proveedores realicen cambios en sus redes con propósitos de seguridad o ingeniería, y en algunos casos, puede prohibir o disuadir a los proveedores de brindar acceso a herramientas de cifrado que podrían proteger a las comunicaciones contra las escuchas (ya sea por parte del gobierno o terceros).

También cabe mencionar que la obligación de una empresa de ser capaz de llevar a cabo interceptaciones es distinta de su habilidad para descifrar comunicaciones, o de implementar las tecnologías de cifrado de las cuales no posea las llaves. Sin embargo, puede que los legisladores de la mayoría de las jurisdicciones no hayan considerado de manera expresa estas cuestiones, a las que las Cortes no han puesto a prueba ni examinado.

ARGENTINA: Sobre el cifrado, no hay ninguna ley en Argentina que prohíba el uso de la tecnología de cifrado. Por lo tanto, a través de la aplicación del principio de reserva constitucional que establece que todo lo que no está prohibido está permitido, el cifrado y el uso de tecnología de cifrado es legal en Argentina.

Sobre la interceptación legal, la ley argentina establece varias medidas de seguridad contra registros e incautaciones ilegales. Por un lado, la Ley de Inteligencia Nacional de 2001 establece que todas las intercepciones -ya sea que se lleven a cabo dentro de una investigación criminal o para propósitos de inteligencia- deben ser autorizadas por un juez.[264]

Dicha autorización, según lo establecido por el marco legislativo, "deberá conferirse por escrito y estar justificada por una descripción detallada de cómo van el número de teléfono(s) o e-mail(s) o cualquier otro dispositivo de comunicación va a ser interceptados o

264 Ley 25.520, Article 19.

secuestrado."[265]

Las órdenes de interceptación duran 60 días, pero, a petición, se pueden extender por otros 60 días. La solicitud de intervención debe estar firmada por las autoridades competentes y ser enviada a las empresas de telecomunicaciones y proveedores de servicios de Internet a través de una comunicación oficial, que deberá cumplirse si cumple con los requisitos formales.

La obligación de las empresas intermediarias para cumplir con las órdenes de interceptación se deriva del artículo 22 de la Ley Nacional de Inteligencia de 2001, que establece que estas empresas son "responsables de la ejecución de la desviación [dirigida] de la comunicación." Cabe señalar que no existe una norma que impida a las empresas la implementación de herramientas de cifrado que harían imposible que puedan cumplir con las órdenes de interceptación.

COLOMBIA: Sobre el cifrado: Colombia cuenta con una prohibición legal extremadamente amplia, que data de 1993, sobre todos los usos de la tecnología de cifrado para las comunicaciones en el espectro electromagnético, así como también la prohibición del uso de la tecnología de cifrado de voz para individuos que no fueren determinados funcionarios del gobierno. Al parecer, estas prohibiciones aplican prácticamente a todos los usos de rutina del cifrado en las tecnologías de comunicaciones actuales, pero las leyes no parecen ejecutarse en la práctica.

Sobre la interceptación legal: El decreto 1704 obliga a los servicios de telecomunicaciones (incluyendo a los Proveedores de Servicios de Internet) como Movistar y Claro y a los proveedores de redes a habilitar escuchas más fáciles imponiendo requisitos sobre capacidad técnica, apoyando los estándares técnicos aprobados por el gobierno para las categorías de interceptación de datos, y entregando datos a la Fiscalía General de la Nación cuando así lo solicite.[266] Los proveedores de contenidos y aplicaciones como MercadoLibre.com y Tapssi.com quedan fuera de este decreto.[267]

Los proveedores de redes de telecomunicaciones y de servicios que ejerzan sus actividades dentro del territorio nacional están obligados a garantizar la infraestructura tecnológica necesaria para brindarles la conexión y los puntos de acceso a las autoridades competentes para capturar el tráfico de las comunicaciones en sus redes están implementados, con el objetivo de que las agencias que cumplan las funciones de la policía judicial puedan llevar a

265 Ley 25.520, Article 18.

266 Colombia, Decreto 1704 de 2012, artículo 2.

267 El artículo 6 de la Ley 1341 de 2009 requiere al Ministerio de Tecnología de la Información y Comunicación que cree un glosario. La Resolución 000202 de 2010, crea el glosario y define que las empresas de Internet se consideran proveedores de contenidos y aplicaciones, y no proveedores de telecomunicaciones.

cabo todas las actividades requeridas para la interceptación de las comunicaciones, previa autorización del Fiscal General o de la persona que este designe.

Los proveedores de servicios y de redes de telecomunicaciones deben, además, responder con rapidez a las solicitudes de interceptación de las comunicaciones que presente el Fiscal General, de conformidad con este decreto y el marco legal vigente al día de hoy, para facilitar las actividades de interceptación de las agencias permanentes de la policía judicial.

Adicionalmente, el Ministerio de Tecnologías de la Información y las Comunicaciones puede, de ser necesario, definir las especificaciones técnicas de los puntos de conexión y el tipo de tráfico por interceptar, e imponer, mediante resoluciones generales, condiciones técnicas y modelos, así como también protocolos sistemáticos que deberán seguirse, a los proveedores de servicios y redes de telecomunicaciones, en respuesta a las solicitudes de interceptación del Fiscal General.

EL SALVADOR: Sobre el cifrado: El artículo 42-D de la ley de telecomunicaciones señala que los proveedores de telecomunicaciones "deberán descriptar o asegurar que las autoridades puedan descriptar cualquier información de un suscriptor o cliente, con el propósito de obtener la información a la que se refieren los dos artículos anteriores, en los casos en que la encriptación haya sido proveída por el operador del servicio". Esto se puede interpretar como una prohibición para los proveedores de emplear o brindar tecnologías de cifrado que ellos no puedan descifrar, y no queda claro si las compañías pueden recibir una sanción por no entregar información que no poseen.

NICARAGUA: Sobre la interceptación legal: En el capítulo VIII, el artículo 65 de la "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados" crea la obligación tecnológica de diseñar sus servicios de manera que la vigilancia se vea facilitada, e indica que:

> *[L]as empresas privadas o públicas prestadoras de los servicios de comunicación telefónica, informática o de otra naturaleza electrónica [...] deberán prestar todas las condiciones y facilidades materiales y técnicas necesarias para que las intervenciones sean efectivas, seguras y confidenciales [...].*

Sobre el cifrado: No existen limitaciones legales o reglamentarias sobre el cifrado de las comunicaciones o del contenido.

BRASIL:[268] La Constitución de Brasil prohíbe de manera expresa el anonimato. La ley no

268 Extracto de las Preguntas Frequentes elaboradas por el Electronic Frontier Foundation & Internet Lab para este investigacion (2015). https://necessaryandproportionate.org/country-reports/brazil

permite el uso del cifrado en Brasil.[269] Sin embargo, la Agencia Nacional de Telecomunicaciones de Brasil (ANATEL) exige que los prestadores de telecomunicaciones cuenten con los recursos y las instalaciones necesarias para violar la secrecía de las comunicaciones dentro del alcance de las órdenes judiciales. La ANATEL también dicta que los proveedores corran con los gastos de manutención de dicha tecnología (art. 26, párrafo único, Resolución nº 73/98; art. 90, Resolución nº 477/07; art. 24, Resolución nº 426/05). La Ley de Interceptación Brasilera obliga a los proveedores de telecomunicaciones a cooperar con las agencias de aplicación de la ley en los procedimientos de escuchas autorizados por ley (art. 7, Ley nº. 9.296/96). Aunque se puede interpretar que esta redacción restringe el uso y el tipo de cifrado y tecnologías análogas implementadas por esos agentes, estas obligaciones (al estilo CALEA) no se extienden directamente a los proveedores de contenidos (aplicaciones de terceros, como WhatsApp). La creciente popularidad de conocidas aplicaciones de mensajería cifrada en Brasil, como WhatsApp, ha provocado un debate acalorado acerca del cifrado en el país.

En mayo de 2016, el juez que exigió datos personales a WhatsApp durante una investigación relacionada con el narcotráfico en el estado de Sergipe, ubicado al noreste, ordenó a los cinco proveedores de Internet más importantes bloquear el acceso al servicio de mensajería de WhatsApp por 72 horas. Los PSI que no cumplieron con esta orden recibieron la amenaza de pagar una multa de aproximadamente $142.000 dólares estadounidenses por día.

En febrero de 2016, el mismo juez ordenó el arresto del vicepresidente de Facebook de Brasil, como parte del mismo caso. El arresto se produjo después de que el juez haya notificado a WhatsApp (que pertenece a Facebook) sobre una serie de multas por rehusarse a entregar información a la corte. El vicepresidente de Facebook fue liberado[270]después de que otro juez brasilero denominó su detención como "coerción ilegal". El abogado de WhatsApp reveló a la prensa[271] lo que dijo en la corte: WhatsApp no puede brindar el contenido de las comunicaciones transmitidas mediante su servicio de mensajería, ya que la compañía no posee registro de tales comunicaciones. Esto puede ocurrir por razones tecnológicas — muchas comunicaciones de WhatsApp están cifradas de extremo a extremo. También puede ser el resultado de las políticas de registro de la compañía: WhatsApp afirma que no lleva registros permanentes[272] de los datos que solicita la corte. Sea como fuere, la corte pretendía

269 Dennys Antonialli, Jacqueline de Souza Abreu, "Brasil: Vigilancia Estatal de las Comunicaciones en Brasil y la Protección de los Derechos Fundamentales", Electronic Frontier Foundation & InternetLab (2015). https://necessaryandproportionate.org/country-reports/brazil

270 Brazil judge orders release of Facebook executive, https://www.yahoo.com/news/brazil-judge-orders-release-facebook-executive-130638549.html?ref=gs

271 Sergio Rodas, Executivo do Facebook é preso por causa de apuração envolvendo WhatsApp, Revista Consultor Jurídico (2016). http://www.conjur.com.br/2016-mar-01/executivo-facebook-preso-causa-apuracao-envolvendo-whatsapp

272 Apesar de problemas judiciais, WhatsApp diz que não vai mudar (2016) http://www1.folha.uol.com.br/tec/2016/03/1745230-apesar-de-problemas-judiciais-

sancionar a un solo empleado por la incapacidad de la compañía para cumplir con las imposibles exigencias de la corte. En diciembre de 2015, se les solicitó a los PSI brasileros que bloqueen el acceso a WhatsApp durante un caso diferente en São Paulo, orden que fue rápidamente anulada tras un recurso de amparo.

GUATEMALA: Sobre el cifrado: No existen limitaciones legales o reglamentarias sobre el desarrollo y uso del cifrado.

HONDURAS: Sobre el cifrado: No existe regla constitucional que rija la promoción o limitación del cifrado o el anonimato. La Sala Constitucional de la Suprema Corte no ha abordado ninguna de estas cuestiones. No obstante, la Ley de Intervención de las Comunicaciones es, potencialmente, ambigua con respecto a las obligaciones de interceptación de los proveedores de servicios. Exige que los proveedores de servicios de comunicaciones pongan "todas las facilidades materiales, técnicas y humanas para que las intervenciones sean efectivas, seguras y confidenciales" a disposición de las entidades del gobierno; no queda claro hasta qué punto esto impediría a los proveedores adaptar o promover las herramientas de seguridad y cifrado que limitan su propio acceso a las comunicaciones de sus usuarios.

PERÚ: Sobre el cifrado: No existen limitaciones legales o reglamentarias sobre el desarrollo y uso del cifrado.

Sobre la interceptación legal: el artículo 230 del Código Procesal Penal deja en claro que los PSI deben mantener sus sistemas "en proximidad inmediata a" la policía para facilitar la ejecución de cualquier orden de vigilancia. De acuerdo con esta regla, cualquier tipo de medida anti-vigilancia empleada por los PSI puede interpretarse como una violación a esta obligación:

> *4. Las empresas telefónicas y de telecomunicaciones deberán inmediatamente brindar la geolocalización de los teléfonos celulares y deberán posibilitar la diligencia de intervención y grabación o registro de las comunicaciones cuando medie orden judicial, en tiempo real, de manera continua, las 24 horas al día, los 365 días del año, bajo apercibimiento de ser denunciados por delito de desobediencia a la autoridad. Los encargados de realizar la diligencia y los servidores de las indicadas empresas deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento.* Estas empresas le concederán a la Policía Nacional de Perú el acceso a su tecnología y garantizarán su compatibilidad e interconexión con el Sistema de Intervención y Control de las Comunicaciones de la policía nacional. Además, cuando por razones de innovación tecnológica, las empresas actualicen sus equipos y software, quedarán obligadas a asegurar que la nueva tecnología continúe siendo compatible con el Sistema de Intervención y Control de las Comunicaciones*

whatsapp-diz-que-nao-vai-mudar.shtml

*de la Policía Nacional de Perú.**

Por otro lado, los PSI tienen la responsabilidad general de hacer cuanto puedan para proteger las comunicaciones de sus usuarios, por ejemplo, brindando o permitiendo el uso de comunicaciones de extremo a extremo. Esta obligación claramente supone que no podrían prohibir que sus usuarios usen cifrado de extremo a extremo.

CHILE: Sobre el cifrado: No existen limitaciones legales o reglamentarias sobre el desarrollo y uso del cifrado.

Sobre la interceptación legal: Los operadores en Chile deben cooperar con las órdenes de escuchas telefónicas, mantener la capacidad técnica para llevarlas a cabo, e informar a la autoridad de Telecomunicaciones sobre el tipo de tecnología que poseen para hacerlo. No se les prohíbe utilizar herramientas de confidencialidad.

MÉXICO: Sobre el cifrado: No existen limitaciones legales o reglamentarias sobre el desarrollo y uso del cifrado. No se les prohíbe a las compañías utilizar herramientas de cifrado.

9.
Garantías contra el acceso ilegítimo y derecho a recurso efectivo

En el derecho penal, algunos estados de la región definen varios delitos por el acceso a las comunicaciones sin autorización o por la divulgación arbitraria de comunicaciones o datos personales. Generalmente, las leyes imponen sanciones por la interceptación ilegal o la divulgación indebida de información privada, y establecen recursos para subsanar tales ofensas.

PERÚ, BRASIL, Y ARGENTINA: La ley peruana 27.697 señala que los participantes en el proceso de investigación (el juez, personal de los tribunales, el fiscal, personal de apoyo, la Policía Nacional, peritos, y otras personales naturales o jurídicas autorizadas) deben mantener la confidencialidad de la información obtenida como resultado de la interceptación de las comunicaciones. El mismo deber de confidencialidad se aplica en Brasil[273] y Argentina.[274]

En el ámbito de la inteligencia, la legislación de inteligencia de Argentina impone sanciones penales a los miembros de los servicios de inteligencia que indebidamente intercepten, capturen o desvíen el curso de las comunicaciones que no estén dirigidas a ellos.[275] En 2015, la Ley No. 25.520 de Inteligencia Nacional incorporó disposiciones penales para sancionar a aquellos que, permanente o transitoriamente, participen en las tareas que regula esta ley: en caso de que "indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos".[276]

Esta ley también impone sanciones penales a aquellos que, contando con una orden judicial y obligados a hacerlo, "omitieren destruir o borrar los soportes de las grabaciones, las copias de las intervenciones postales, cablegráficas, de facsímil o de cualquier otro elemento que permita acreditar el resultado de las interceptaciones, captaciones o desviaciones".[277]

273 República de Brasil, Ley 9.296 de 1996, artículo 8.

274 República Argentina, Código Procesal Penal Nacional, artículo 143.

275 República Argentina, Ley No. 25.520 de Inteligencia Nacional, Boletín Oficial del 6 de diciembre de 2001, artículo 42.

276 República Argentina, Ley No. 25.520 de Inteligencia Nacional, Boletín Oficial del 6 de diciembre de 2001, artículo 42.

277 Ibíd, artículo 43.

Además, según esta ley, aquellos funcionarios públicos o funcionarios del gobierno que realicen actividades de inteligencia prohibidas por esta ley, también deberán ser sancionados.[278]

Además, en la legislación argentina sobre los servicios de vigilancia, no existen incentivos para que los agentes de inteligencia divulguen publicamente información sobre prácticas que vulneran los derechos fundamentales.[279]

Si bien existen garantías formales, no existen casos conocidos de agentes de inteligencia que han sido - efectivamente - castigados, por violar ilegalmente comunicaciones privadas de los ciudadanos, por los órganos de inteligencia en si mismos o por los organismos que los supervisan. Existen casos en que el Poder Judicial ha encontrado infracciones ilegales, pero en el contexto de una demanda civil que dio lugar a la concesión de daños.[280]

COLOMBIA: El derecho penal detalla una serie de delitos relacionados con la vigilancia ilegal de las comunicaciones, incluyendo la interceptación de las comunicaciones sin que medie una orden. Sin embargo, el artículo 250 de la Constitución permite a la Fiscalía General interceptar las comunicaciones con un control judicial posterior, lo que crea un sendero para que se aborden las violaciones que existieren. Adicionalmente, la reforma del Código Penal aprobada en 2009 para la protección de la información de los individuos, añadió un nuevo título al código, el cual describe delitos, incluyendo el acceso abusivo a un sistema informático, la interferencia ilegítima de sistemas informáticos o redes de telecomunicaciones, la interceptación de datos, y daños informáticos, y el uso de malware y ataques de *spoofing* para la captura de datos personales.[281]

CHILE: El derecho penal chileno incluye sanciones para aquellos que violen el derecho a la privacidad. El Decreto sobre Servicios de Telecomunicaciones No. 18, de enero de 2014, penaliza la interceptación o captura maliciosa sin autorización de cualquier tipo de señal. Las sanciones de privación de la libertad y multa empeoran cuando existe una transmisión pública o privada del contenido de dichas señales. El artículo 161-A del Código Penal penaliza a aquellos que, sin permiso, capturan, graban, o interceptan conversaciones privadas. La sanción incluye una menor multa o privación de la libertad, pero aumenta en los casos en que el delincuente haya difundido las conversaciones obtenidas.

Cuando la vigilancia ocurre con arreglo a la ley, esta exige que las compañías de

278 Ibíd, artículo 43 b.

279 Vea Bertoni, Eduardo. "Ley de inteligencia, oportunidad perdida", Bastión Digital, (2015). http://ar.bastiondigital.com/notas/ley-de-inteligencia-oportunidad-perdida#sthash.Td5djgJU.dpuf.

280 National Court of Appeals in Administrative Matters. Case of Ventura, Adrián c. Estado Nacional EMGFFAA s/ daños y perjuicios. Decision of February 28, 2008 (p. viii).

281 República de Colombia, Ley 1273 de 2009.

telecomunicaciones guarden silencio al tomar conciencia de alguna actividad de vigilancia de las comunicaciones, salvo que se les solicite declarar en el procedimiento penal. No se conoce, sin embargo, qué sanciones son aplicables en caso de no cumplimiento de este deber. Esta última disposición puede significar un problema para el principio de notificación del usuario; analizamos esto a fondo en la sección dedicada a ese principio.

10.
Recomendaciones Finales

Muchas leyes de vigilancia de la región son difíciles de entender porque varias de las disposiciones relevantes están dispersas en muchas y distintas leyes que planean cubrir una serie de cuestiones y no solamente la vigilancia. Para minimizar este problema, los países deberían contar con una ley de vigilancia integral en vez de tener varias disposiciones dispersas en diferentes leyes, resoluciones y decretos.

Las leyes de vigilancia no deberían hacer distinciones arbitrarias entre los diversos tipos de información protegida, como el contenido, los metadatos, la geolocalización, los datos del suscriptor, los datos retenidos, y las comunicaciones en tiempo real. En cambio, solamente debería permitirse el acceso a cualquier tipo de información protegida cuando, como mínimo, un juez imparcial haya emitido una orden basada en la necesidad, la proporcionalidad, la idoneidad y el objetivo legítimo de la medida solicitada. Además, los países de la región deben adoptar las salvaguardas legales como el debido proceso, la transparencia, la supervisión pública, la notificación, y el derecho a recurso efectivo.

Recomendaciones relacionadas con cada principio en particular

1. Con respecto al principio de legalidad

Al regular el acceso y recopilación de información protegida y personal, los Estados tienen el deber de promulgar una legislación clara, que no pueda interpretarse de manera arbitraria. Por este motivo, sugerimos lo siguiente:

1. Brasil debería modificar el artículo 21 de la Ley de Organizaciones Criminales No. 12.850, la que penaliza la negativa o inobservancia de entregar "información de la cuenta, registros, documentos, e información solicitada por el juez, el Ministerio Público, o el delegado de la policía civil durante una investigación o proceso" e impone sanciones que van desde los seis meses hasta los dos años de privación de la libertad. El artículo 21 creó confusión acerca de cuándo se necesita una orden. Brasil también debería modificar el artículo 17 de la Ley 12.850 para fijar límites estrictos a la retención de datos obligatoria para las compañías de telecomunicaciones.

2. Colombia debería modificar el Decreto 1704 de 2012 para aclarar que las compañías telefónicas y de telecomunicaciones no están obligadas a retener información que no necesiten para los propósitos del ejercicio de sus actividades.

3. El Salvador debería derogar el artículo 31 de la Ley Especial para la Intervención de las Telecomunicaciones y elaborar una norma que determine de manera pública el

procedimiento de interceptación de las telecomunicaciones. Del mismo modo, Perú debería promulgar una norma que detalle el procedimiento para el acceso a los datos de geolocalización de teléfonos celulares y aparatos electrónicos para que el alcance y las bases de la autoridad del gobierno se conozcan públicamente.

4. Guatemala debería modificar el artículo 48 de la Ley contra la Delincuencia Organizada para especificar el tipo de comunicaciones que pueden ser interceptadas.

5. Honduras debe modificar los artículos 3 y 10 de la Ley de Intervención de las Comunicaciones para que indiquen explícitamente los tipos de técnicas y tecnologías de vigilancia que están permitidos o prohibidos actualmente.

6. Asimismo, Chile, Paraguay, Guatemala, y Uruguay deberían eliminar los vacíos legales en sus legislaciones (como el artículo 200 del Código Procesal Penal de Paraguay) cuya interpretación puede tomarse como una autorización de cualquier método de vigilancia que se pueda desarrollar en el futuro. Deberían aclarar qué técnicas y tecnologías son legales, y bajo qué circunstancias pueden o no ser usadas. Algunos Estados deberían dejar de utilizar *software* malicioso con propósitos de espionaje de inmediato, debido a que sus leyes no autorizan su uso.

7. Los Estados deberían mantener audiencias públicas para examinar si ya están en uso en sus territorios los recolectores IMSI o cualquier otra nueva forma de tecnologías de vigilancia, y para saber cuáles son las entidades que las están utilizando. En los lugares en que dichos aparatos estén en uso, las legislaciones deberían actualizarse para abordarlos de manera que cumplan con los 13 Principios de Necesidad y Proporcionalidad. Las actualizaciones deberían incluir requisitos con respecto a la autorización judicial y la supervisión pública, así como también obligaciones de transparencia para evitar abusos de poder. (Por ejemplo, dicha ley debe garantizar que la recopilación de cualquier dato mediante simuladores de torres de telefonía debe estar autorizada por una orden emitida por un juez neutral, basada en la necesidad, proporcionalidad, idoneidad y objetivo legítimo). En general, los Estados deben asegurar que las nuevas tecnologías de vigilancia invasiva estén controladas por la ley de una manera que históricamente sea más firme que técnicas como las escuchas telefónicas, y garantizar que la cultura del secreto y el vacío jurídico no rodeen a las nuevas tecnologías.

2. Con respecto al principio de objetivo legítimo

Todos los Estados de la región deberían restringir las circunstancias bajo las cuales se autoriza la vigilancia de las comunicaciones (aparte de las escuchas telefónicas, esto incluye todas las formas de vigilancia, como la localización de dispositivos y el monitoreo de los metadatos). Por ejemplo, los Estados podrían especificar que la vigilancia de las comunicaciones puede llevarse a cabo, solamente, para la investigación de una determinada lista de delitos graves. Adicionalmente, los Estados podrían limitar la vigilancia al uso probatorio para delitos

graves definidos y asegurar que las medidas de vigilancia únicamente procedan cuando exista una sospecha fundada de que la vigilancia pueda producir evidencia admisible.

Los Estados como Honduras, que no limitan el alcance las actividades de vigilancia en este sentido, deberían modificar sus legislaciones para cumplir con este requisito.

3. Con respecto al principio de necesidad

Los Estados de la región deberían autorizar el uso de la vigilancia de las comunicaciones solamente cuando sea la única manera de lograr el objetivo legítimo o cuando sea el medio menos propenso a vulnerar los derechos humanos. Siguiendo el ejemplo de Brasil, los Estados deberían especificar que un juez no puede autorizar la interceptación de las comunicaciones cuando la evidencia que se desea conseguir puede obtenerse mediante otros medios. También es una buena práctica delimitar los casos en los que las autoridades no pueden realizar determinadas actividades de vigilancia de las comunicaciones, bajo ninguna circunstancia.

4. Con respecto al principio de idoneidad

Los Estados de la región deberían limitar el uso de la vigilancia de las comunicaciones a los casos en que haya una sospecha fundada de que una persona es la responsable de un crimen y que la vigilancia sería útil en la investigación de dicho crimen.

5. Con respecto al principio de proporcionalidad

Los Estados de la región deberían adoptar distintas reglas que equilibren de una manera justa el objetivo legítimo perseguido por la vigilancia de las comunicaciones y los derechos fundamentales afectados por estas actividades. Específicamente, los Estados deberían:

1. Exigir que cualquier información remanente que se haya recopilado con el propósito de vigilancia sea destruido o devuelto con prontitud.

2. Exigir que los jueces emitan, unicamente, órdenes extremadamente detalladas en cuanto a las autorizaciones de vigilancia de comunicaciones, garantizando que los jueces conozcan y examinen los detalles de las actividades de vigilancia propuestas (desde los objetos de vigilancia y los métodos, hasta los objetivos y plazos).

3. Restringir el uso de la vigilancia de las comunicaciones a casos en los que exista un alto grado de certeza de la comisión de un crimen.

4. Adoptar medidas, como las de selección de objetivos y minimización para limitar el impacto de los métodos de vigilancia técnica en las personas y dispositivos que no sean los destinados a vigilar.

5. Fijar plazos para la interceptación de las comunicaciones. Estados como el de Brasil, cuya legislación establece que las órdenes de escucha pueden renovarse de manera

indefinida, deberían modificar estas disposiciones.

6. Rechazar las leyes de retención de datos que obligan a los PSI y prestadores de servicios de telecomunicaciones a retener datos del suscriptor y de llamadas telefónicas o los metadatos de la totalidad de la población para el posible uso por parte de las agencias de aplicación de la ley. México, Perú, Chile, Brasil, Paraguay, Colombia, y Honduras deberían derogar las leyes que requieran dicha retención. La Unión Europea ha determinado que las leyes de retención de datos violan los derechos a la privacidad, pero América Latina no ha hecho mucho progreso en ese sentido.

6. Con respecto al principio de autoridad judicial competente

Los Estados de la región deberían exigir que las autoridades judiciales reexaminen las injerencias en el derecho a la inviolabilidad de las comunicaciones. Como regla general, la revisión judicial debería ocurrir antes de la vigilancia de comunicaciones personales. Exclusivamente en casos de emergencia, cuando la vida o integridad física de un individuo esté en peligro, la revisión judicial podría darse después de que el derecho a la inviolabilidad de las comunicaciones haya sido vulnerado. En todos los casos en que la revisión judicial sea posterior, esta debe ocurrir inmediatamente después de dicha injerencia. Los Estados deberían aclarar que cada acto de vigilancia específico precisa una autorización judicial diferente, y que la renovación o expansión de cualquier medida de vigilancia autorizada requiere una nueva aprobación judicial.

Los jueces deberían tener el conocimiento suficiente y recibir la información adecuada para poder comprender los detalles de cada medida de vigilancia propuesta, y su impacto en los sistemas de comunicaciones. Por ejemplo, los jueces pueden desconocer que los volcados de torres *(tower dumps, en inglés)*, mediante los que se obtienen los registros de actividades desde la infraestructura celular, inevitablemente incluyen una gran cantidad de datos de terceros que son inocentes, y que no son las personas previstas para la vigilancia. Consecuentemente, los Estados deberían explorar la idea de obtener la ayuda de expertos técnicos independientes para instruir a los jueces.

7. Con respecto al principio de debido proceso

Los Estados de esta región deberían incorporar el debido proceso, por lo menos, decretando que los documentos privados obtenidos sin una orden judicial y sin las salvaguardas legales que correspondan carecerán de efecto jurídico. También deberían tomar medidas para evitar los arreglos informales, incluyendo la cooperación voluntaria en la vigilancia entre el sector privado y el gobierno para facilitar la vigilancia de las comunicaciones; en cambio, la vigilancia debería llevarse a cabo de conformidad con las solicitudes formales presentadas con arreglo a la ley.

8. Con respecto al principio de notificación del usuario

Los Estados de la región deberían incorporar en las leyes una obligación para la notificación de aquellos que se vean afectados directamente por la vigilancia. Puesto que deberán existir excepciones para la entrega de dicha notificación, la ley deberá explicar en detalle cuáles son estas y deberá exigir que se acuda a ellas lo menos posible. Las entidades que soliciten la vigilancia deben brindar las razones por las que la notificación puede ser diferida en casos particulares.

Cuando la secrecía de la vigilancia sea necesaria para un interés convincente del gobierno, la ley debe prever cómo y cuándo tal secreto tendrá un fin y cómo se notificará eventualmente a los sujetos de vigilancia y a otras personas afectadas por esta y, cuando proceda, qué recurso obtendrán en contra de la vigilancia ilegal.

9. Con respecto al principio de transparencia

Los Estados de la región deberían promulgar leyes que incentiven a las compañías a maximizar la cantidad de información que revelan al público sobre sus capacidades y prácticas de vigilancia. Esa transparencia ayudará a que los ciudadanos puedan hacer que los gobiernos rindan cuentas de sus actos. La Ley General de Transparencia y Acceso a la Información Pública de México incentiva a los prestadores a publicar información acerca de las solicitudes de información que presenta el gobierno. Pueden seguir este ejemplo, cuya ley motiva a las compañías a brindar información sobre los pedidos de datos presentados por el gobierno.

Las empresas deberían publicar informes de transparencia de manera voluntaria que muestren estadísticas sobre la naturaleza y el alcance de su interacción con el gobierno y la participación en las actividades de vigilancia.

10. Con respecto al principio de supervisión pública

Los Estados de la región deberían implementar mecanismos de supervisión pública para controlar posibles abusos de poder en lo que respecta a la vigilancia de las comunicaciones. La supervisión privada dentro de los gobiernos no puede sustituir a la supervisión pública.

Anexo I

Protecciones constitucionales contra la vigilancia de las comunicaciones

Todos los países que se analizan en este estudio poseen constituciones que protegen el derecho a la vida privada y, en particular, a la inviolabilidad de las comunicaciones.

La constitución mexicana, como muchas otras constituciones modernas, reconoce de manera explícita el derecho a la protección de los datos en el artículo 6:

> *La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes [...].*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*[282]

El artículo 16 enumera detalladamente varias protecciones para la privacidad de las comunicaciones, y se incluyen las siguientes:

> *Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandato escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. [...]*
>
> *Las autoridades judiciales son las únicas que pueden emitir una orden de cateo a solicitud del Ministerio Público. La orden de cateo debe expresar el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan.*

282 Const. de México, art. VI, § 2 y 3.

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

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. [L]a autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de esta y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor [...].

Los poderes judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los derechos de los indiciados y de las víctimas u ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes.

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio [...].[283]

Al interpretar el artículo 16, la Suprema Corte de Justicia, en el Amparo 1.621/2010 de 2011, indicó que el derecho a la inviolabilidad de las comunicaciones protege tanto el contenido de las comunicaciones como los datos relacionados con dichas comunicaciones:

A fin de garantizar la reserva que se predica de todo proceso comunicativo privado, resulta indispensable que los datos externos de la comunicación también sean protegidos. Si bien es cierto que los datos no se refieren al "contenido" de la comunicación, también lo es que en muchas ocasiones ofrecen información sobre las circunstancias en que se ha producido la comunicación, afectando así, de modo directo o indirecto, la privacidad de los comunicantes. [...] Así, a modo ejemplificativo, el registro de los números marcados por un usuario de la red telefónica, comunicantes o la duración de la llamada telefónica, llevado a cabo sin las garantías necesarias para la restricción del derecho fundamental al secreto de las

283 Const. de México, art. XVI.

comunicaciones, puede provocar su vulneración".[284]

En otro caso (Contradicción de tesis 194/2012), la Suprema Corte respondió la siguiente pregunta legal sobre privacidad:

> *¿Constituye o no una violación a la intervención de comunicaciones privadas, preservada en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el que la autoridad ministerial o los agentes a su mando revisen, extraigan o utilicen como medio de prueba los archivos electrónicos almacenados en forma de texto, audio, imagen o video, del teléfono celular que traía consigo el detenido relacionado con la comisión de un delito?*

En su respuesta, la Suprema Corte, en la Contradicción de Tesis 194/2012 dejó en claro que el acceso y el análisis de los datos almacenados en un teléfono celular sin que medie una autorización judicial representan una violación al derecho a la inviolabilidad de las comunicaciones privadas:

> *En términos del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para intervenir una comunicación privada se requiere autorización exclusiva de la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, por lo que todas las formas existentes de comunicación y las que son fruto de la evolución tecnológica, incluso del teléfono celular [...], deben protegerse por el derecho fundamental a su inviolabilidad. [Además] el acceso y análisis de los datos contenidos en un teléfono móvil sin contar con una autorización judicial constituye una violación al derecho a la inviolabilidad de las comunicaciones privadas.*[285]

Asimismo, en el caso 1.621/2010 (Amparo en revisión), la Suprema Corte señaló que las comunicaciones privadas son inviolables, sin importar cuál sea su contenido. Además, indicó que la información que identifica a una comunicación, como los números que marca el usuario, la identidad de quienes llaman, la duración de la llamada o en el caso de que sea un email, la dirección IP, también se protegerá. La Suprema Corte también hizo hincapié en que la protección de las comunicaciones privadas persiste con el correr del tiempo, y así, acabada una comunicación, el medio por el cual se conserva o almacena el contenido de ésta, también se vuelve inviolable. La Suprema Corte también dejó en claro que, para que una comunicación sea inviolable, el mensaje debe transmitirse a través de cualquier medio o aparato técnico que sea un producto tecnológico, ya sea un telégrafo, teléfono, email, o cualquier otro medio que producto de los avances tecnológicos. La Suprema Corte aclaró que se considera que un e-mail es interceptado cuando la contraseña o clave de seguridad se

284 México, Suprema Corte de Justicia, Amparo Directo en revisión 1.621/2010, (15 de junio de 2011).

285 México, Suprema Corte, Sala Primera, Contradicción de Tesis 194/2012.

obtiene sin autorización judicial o sin autorización del dueño de la cuenta, o cuando dicha autorización haya sido revocada.[286]

Recientemente, la Suprema Corte de México cotejó que la obligación de retener los datos de las comunicaciones de los ciudadanos mexicanos "no constituye una limitación a la inviolabilidad de las comunicaciones".[287]

> *[D]e igual modo, la [Suprema Corte de México] no ha considerado que la protección constitucional brindada al contenido de las comunicaciones y a los metadatos se extienda a la ubicación de teléfonos celulares en tiempo real. Como ejemplo, se encuentra la decisión de la [Suprema Corte de México] al resolver la acción de inconstitucionalidad 32/2012,[288] en la que la mayoría de la Suprema Corte consideró que una disposición que faculta a la Procuraduría General de la República (PGR) a monitorear la localización geográfica de un teléfono móvil, en tiempo real, sin necesidad de obtener autorización judicial federal era constitucional. De lo anterior, se desprende que a nivel normativo, la Constitución otorga protecciones amplias al derecho a la inviolabilidad de las comunicaciones, no obstante, la interpretación de dichas disposiciones no se extiende a la protección contra la retención de datos masiva o la recopilación de datos de localización de teléfonos móviles.[289]*

El artículo 100 de la Constitución de HONDURAS protege "la inviolabilidad y secreto de las comunicaciones, en especial de las postales, telegráficas, y telefónicas, salvo resolución judicial".[290] Al interpretar esta disposición, la Sala Penal de la Suprema Corte de Honduras dictaminó que la protección constitucional del derecho a la privacidad de las comunicaciones incluye las comunicaciones digitales y telefónicas, aun cuando sean banales, mundanas, o insignificantes. En la misma disposición, la Sala dejó en claro que la protección de la inviolabilidad de las comunicaciones comprende la protección de los registros de cualquier comunicación que estén almacenados en cualquier entidad pública o privada. La Sala indicó que el derecho a la inviolabilidad de las comunicaciones, que se consagra en el artículo 100, deriva del derecho a la vida privada, y agregó que la protección constitucional se extiende a la vigilancia de las comunicaciones en tiempo real o ex post facto:[291]

---

286 México, Suprema Corte, Sala de Primera Instancia, Amparo en Revisión 1.621/2010 y Contradicción de Tesis 194/2012, en las cuales se aclara el alcance de la protección a la privacidad.

287 Suprema Corte. Segunda Sala. Amparo en Revisión 964/2015.

288 Suprema Corte. Sesión Plenaria. Acción de Inconstitucionalidad 32/2012.

289 Para un análisis detallado sobre los problemas legales relacionados con la retención de datos, lea a Luis Fernando García, "México: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México", Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales (2016). https://necessaryandproportionate.org/country-reports/mexico

290 Const. Política de la República de Honduras, art. C.

[L]e Secret Des Lettres es inviolable [...] y la inviolabilidad de las comunicaciones privadas que nuestra Constitución de la República consagra en el artículo 100, derivan del derecho a la vida privada, y prohíbe a los particulares ajenos a la comunicación y principalmente al Estado: el secuestro, la captación, interceptación, apertura, grabación, reproducción o divulgación de una comunicación de carácter privada, sea que dichas acciones se realicen al momento en que la comunicación se esté llevando a cabo (en tiempo real), sea que se realice ex post facto o sea que se realice donde conste el registro de la comunicación, como ser materialmente las cartas, dispositivos de teléfonos o computadoras, o electrónicamente en las cuentas personales de e-mails, buzones de redes sociales, chats, etc. [...] La inviolabilidad de las comunicaciones incluye la protección de los registros que llevan las empresas públicas o privadas.[292]

La Constitución de EL SALVADOR también garantiza la protección de las comunicaciones. El artículo 24 contiene dos partes: la primera parte reconoce la inviolabilidad de la correspondencia; la segunda explica las excepciones posibles a esta protección:

La correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las comunicaciones telefónicas.

De manera excepcional podrá autorizarse judicialmente, de forma escrita y motivada, la intervención temporal de cualquier tipo de telecomunicaciones, preservándose en todo caso el secreto de lo privado que no guarde relación con el proceso. La información proveniente de una intervención ilegal carecerá de valor [...].[293]

La Constitución de la República Federativa de BRAZIL protege la inviolabilidad de la intimidad, la vida privada, y el domicilio. Esto incluye la protección de la privacidad de la correspondencia, de las comunicaciones telegráficas, y de las telefónicas, salvo exista una orden judicial para examinar las comunicaciones con el objetivo de llevar a cabo una investigación criminal.[294] También se protege el derecho a habeas data, teniendo en cuenta que el acceso a los datos será concedido en los siguientes casos:

1. para asegurar el conocimiento de informaciones relativas a la persona del solicitante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; y

291 Honduras, Sala en lo Penal, Suprema Corte de Justicia, Sentencia CP-48-2011, 20. http://www.poderjudicial.gob.hn/Jurisprudencia/Documents/CP-48-2011.pdf

292 Honduras, Sala en lo Penal, Suprema Corte de Justicia, Sentencia CP-48-2011, 20. http://www.poderjudicial.gob.hn/Jurisprudencia/Documents/CP-48-2011.pdf

293 Const. de El Salvador, art. XXIV.

294 Const. de la República Federativa de Brasil, art. V, § 10, 11, y 12.

2. para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo.[295]

Lamentablemente, a pesar de que este texto constitucional es favorable, no se le ha hecho una interpretación exhaustiva.

> *[L]os problemas de interpretación ponen en peligro la protección real que dichos derechos brindan en contra de la vigilancia indebida de las comunicaciones por parte de las autoridades estatales. [...] [A pesar de esto,] el derecho a la privacidad (contemplado de manera general bajo el inciso X del mismo artículo) prevé la protección de las comunicaciones en un sentido más amplio,[296] que incluye no sólo el contenido de las comunicaciones, sino también las circunstancias en las que ocurren y entre quiénes (estos datos pueden revelarse a través de la información de la cuenta[297] y los metadatos[298]).*

La Constitución de ARGENTINA reconoce la inviolabilidad del domicilio y de las comunicaciones.[299] Aunque la Constitución se refiere expresamente a las cartas escritas, la Suprema Corte de Justicia de Argentina ha extendido esta protección constitucional a las comunicaciones que se dan a través de Internet.[300] En *Halabi, Ernesto c/ P.E.N.*, por ejemplo, la Suprema Corte dictaminó que Argentina vulneró el derecho a la privacidad con la disposición de la Ley Nacional de Telecomunicaciones de 2003 y su reglamento complementario.

Estas leyes obligaban a las compañías de telecomunicaciones y a los proveedores de servicios de Internet a registrar, indexar, y almacenar el tráfico de datos por un periodo de 10 años y a

295 Const. de la República Federativa de Brasil, art. V, § 72.

296 *Vea* Tribunal Supremo Federal, *Mandado de Segurança* 24.817/DF, caso informado por el Juez Celso de Mello, juzgado el 3 de febrero de 2005, el cual relaciona las violaciones a la confidencialidad de los registros impositivos, bancarios y telefónicos con las restricciones a los derechos contemplados en el artículo X. http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605418

297 A los efectos de este reporte, "información de la cuenta" hace referencia a la información contenida en los registros del usuario en la compañía telefónica, operador de sistema autónomo, o proveedor de aplicación.

298 A los efectos de este reporte, el término "metadatos" hace referencia a todos aquellos datos y registros que se generan de una comunicación dada, distintos del contenido de la comunicación, como, por ejemplo, la fecha, hora, y duración de la comunicación, el emisor, el receptor, la ubicación geográfica del dispositivo, cuando se conozca (tales como los identificadores o las mediciones a través de una estación base de radio), códigos de identificación del dispositivo (como el IMEI), y demás cosas por el estilo.

299 Const. de Argentina, art. XVIII: "[...] El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación [...]."

300 Argentina, Corte Suprema, *Halabi v. Poder Ejecutivo Nacional*, (26 de junio de 2007, 24 de febrero de 2009). http://www.iprofesional.com/notas/78867-Fallo-Halabi-Ernesto-c-PEN---ley-25873---dto-156304-s-amparo-ley-16986

facilitar esta información al Poder Judicial argentino y a la Procuración General de la Nación cuando estos así lo soliciten. La disposición sobre la retención de datos fue anulada debido a su redacción imprecisa. La Corte estimó que la ley suponía una "drástica injerencia en la esfera íntima de los particulares" y puso énfasis en la estrecha relación entre los datos de tráfico y el contenido de la información, y que por lo tanto, tales datos no podían ser retenidos. El fallo también dejó en claro que las normas no brindaban un sistema específico para la protección de las comunicaciones electrónicas contra la acumulación y el procesamiento de datos personales automático.[301]

El artículo 26 de la Constitución de NICARAGUA también contempla el derecho a la privacidad:

> *Toda persona tiene derecho:*
>
> 1. *A su vida privada y a la de su familia;*
> 2. *A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo; y*
> 3. *A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información.*

El artículo 27 garantiza la misma protección para los nicaragüenses y extranjeros:

> *Todas las personas son iguales ante la ley y tienen derecho a igual protección.*
>
> *[...] Los extranjeros tienen los mismos deberes y derechos que los nicaragüenses, con la excepción de los derechos políticos y los que establezcan las leyes.*

Otros países han incorporado protecciones similares en sus constituciones:

- La Constitución De EL PERÚ de 1993 reconoce un listado de derechos, los cuales comprenden el secreto e inviolabilidad de las comunicaciones, del domicilio y de los documentos,[302] de la intimidad personal y familiar, y de la voz y la imagen propias.

---

301 Argentina, Corte Suprema, *Halabi v. Poder Ejecutivo Nacional*, (26 de junio de 2007, 24 de febrero de 2009). http://www.iprofesional.com/notas/78867-Fallo-Halabi-Ernesto-c-PEN---ley-25873---dto-156304-s-amparo-ley-16986

302 Const. de Perú, art. II, § 10: secreto e inviolabilidad de comunicaciones y documentos privados. 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. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los documentos privados obtenidos con violación de este precepto no tienen efecto legal. Los libros, comprobantes y documentos contables y administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación, salvo

La Constitución peruana también garantiza que los servicios informáticos, computarizados o no, públicos o privados, no están habilitados a suministrar informaciones que afecten la intimidad personal y familiar.[303]

- La Constitución de URUGUAY es otra de las que reconoce la inviolabilidad de la correspondencia y de los documentos privados.[304]
- El artículo 36 de la Constitución de PARAGUAY sanciona el derecho a la inviolabilidad del patrimonio documental y de las comunicaciones de las personas.[305]
- La Constitución de GUATEMALA reconoce la protección de la inviolabilidad de la correspondencia, documentos, libros, y domicilio.[306]
- El artículo 15 de la Constitución de COLOMBIA reconoce el derecho a la intimidad personal y familiar, y la inviolabilidad de la correspondencia y otras formas de comunicación privada. Señala especialmente que sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Además, el artículo 28 de la Constitución colombiana estipula que toda persona es libre, y que "nadie puede ser molestado en su persona o familia, ni reducido a prisión o arresto, ni detenido, ni su domicilio registrado, sino en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivo previamente definido en la ley".[307]

La Constitución de CHILE es la única en la región que, de manera sorprendente, deja fuera la protección de datos personales ya sea como un derecho en sí mismo o como parte del derecho a la vida privada.[308]

---

por orden judicial.

303 Const. de Perú, art. II, § 6, 7, y 9.

304 Const. de Uruguay, art. XXVIII: "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general".

305 Const. de Paraguay, art. IIIVI. http://www.bacn.gov.py/constitucion-nacional-de-la-republica-del-paraguay.php

306 Const. de Guatemala, art. XXIII y XXIV: "La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna".

307 Const. de Colombia, art. XXVIII.

308 Nelson Remolina, Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales* 1 (no. 1). (2012). http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf citada anteriormente por Valentina Hernández y Juan Carlos Lara, en Vigilancia estatal de las comunicaciones y la protección de derechos fundamentales en Chile,

El derecho a la privacidad se encuentra protegido expresamente en las constituciones de América Latina, ya sea como el derecho a la vida privada, el derecho a la privacidad/intimidad, la protección de datos personales y habeas data, o a la privacidad e inviolabilidad de las comunicaciones, el domicilio, y documentos. Aun así, son pocas aún las resoluciones judiciales en relación con este tema, y el derecho a la privacidad continuará en desarrollo a medida de que se emitan más resoluciones.

Electronic Frontier Foundation & Derechos Digitales, (2016). https://necessaryandproportionate.org/country-reports/chile

Anexo II

El poder normativo de los tratados internacionales de derechos humanos

En América Latina, los estándares internacionales de derechos humanos son claves para el análisis de la legalidad de las prácticas de vigilancia de las comunicaciones por parte del estado. Los tratados internacionales de derechos humanos establecen el núcleo de los derechos humanos y exponen las circunstancias en las que pueden restringirse o limitarse cuando el Estado lleva a cabo la vigilancia de las comunicaciones. El fundamento jurídico de los tratados internacionales de derechos humanos puede encontrarse generalmente en la constitución de cada país. En algunos casos, las cortes constitucionales de los países reconocen y desarrollan con más profundidad la condición legal de los tratados internacionales de los derechos humanos.[309]

Sin perjuicio de cómo se incorporan a cada marco legal interno, los estados que hayan ratificado los tratados internacionales de derechos humanos están obligados a cumplir con las obligaciones internacionales que imponen, de acuerdo con el artículo 26 de la Convención de Viena sobre el Derechos de los Tratados.

Del mismo modo, la Corte Interamericana de Derechos Humanos (Corte IDH) puede ejercer un "control de convencionalidad", mecanismo por el cual los jueces nacionales e interamericanos evalúan la compatibilidad de las prácticas y los instrumentos jurídicos nacionales con la Convención Americana sobre Derechos Humanos. El artículo 62 de la Convención Americana especifica que los estados que hayan ratificado la convención pueden declarar que esta reconoce la jurisdicción de la Corte Interamericana de Derechos Humanos en la interpretación y aplicación de la convención.

La Corte IDH, en *Aguado-Alfaro et al. vs. Perú*, explicó que los jueces nacionales están sujetos a los tratados internacionales ratificados por el estado y deberán ejercer el control de convencionalidad *ex officio* entre las leyes internas y la Convención Americana:

> *128. [C]uando un Estado ha ratificado un tratado internacional como la*

309 Para un análisis pormenorizado, lea a Gongora Mera y Manuel Eduardo, La difusión del bloque de constitucionalidad en la jurisprudencia latinoamericana y su potencial en la construcción del ius constituionale commune latinoamericano, (Instituto de Investigaciones Jurídicas, Instituto Max Planck de Derecho Público Comparado y Derecho Internacional, 2014), http://www.corteidh.or.cr/tablas/r31277.pdf. Vea también Nash Rojas, Claudio, Derecho internacional de Los derechos humanos en Chile: Recepción y aplicación en el ámbito interno, (Facultad de Derecho, Universidad de Chile, septiembre de 2012), http://www.cdh.uchile.cl/media/publicaciones/pdf/91.pdf

Convención Americana, sus jueces también están sometidos a ella, lo que les obliga a velar por que el efecto útil de la Convención no se vea mermado o anulado por la aplicación de leyes contrarias a sus disposiciones, objeto y fin. En otras palabras, los órganos del Poder Judicial deben ejercer no sólo un control de constitucionalidad, sino también "de convencionalidad"[310] *ex officio entre las normas internas y la Convención Americana, evidentemente en el marco de sus respectivas competencias y de las regulaciones procesales correspondientes.*[311]

La Corte IDH, en *Almonacid-Arellano et al vs. Chile*, también afirmó que los jueces y las cortes nacionales están obligados por la Convención Americana:

124. [L]a Corte es consciente [de] que los jueces y tribunales internos están sujetos al imperio de la ley y, por ello, están obligados a aplicar las disposiciones vigentes en el ordenamiento jurídico. Pero cuando un Estado ha ratificado un tratado internacional como la Convención Americana, sus jueces, como parte del aparato del Estado, también están sometidos a ella. [Esto] les obliga a velar porque los efectos de las disposiciones de la Convención no se vean mermadas por la aplicación de leyes contrarias a su objeto y fin, y que desde un inicio carecen de efectos jurídicos. En otras palabras, el Poder Judicial debe ejercer una especie de "control de convencionalidad" entre las normas jurídicas internas que aplican en los casos concretos y la Convención Americana sobre Derechos Humanos. En esta tarea, el Poder Judicial debe tener en cuenta no solamente el tratado, sino también la interpretación que del mismo ha hecho la Corte Interamericana, intérprete última de la Convención Americana.[312]

No sólo los jueces nacionales, sino también todas las ramas del Estado que han ratificado la Convención Americana están sujetos a ella. En *Yatama vs. Nicaragua*, la Corte IDH ordenó que el Estado de Nicaragua garantice que su legislación interna cumpla con las disposiciones de la Convención Americana de Derechos Humanos.

170. [E]l deber general del Estado de adecuar su derecho interno a las disposiciones de dicha Convención para garantizar los derechos en ella consagrados, establecido en el artículo 2, incluye la expedición de normas y el desarrollo de prácticas conducentes a la observancia efectiva de los derechos y libertades consagrados en la misma, así como la adopción de medidas para suprimir las normas y prácticas de cualquier naturaleza que entrañen una violación a las garantías previstas en la

310 Corte Interamericana de Derechos Humanos, Caso de Almonacid Arellano et al., párrafo 124, http://www.corteidh.or.cr/docs/casos/articulos/seriec_154_ing.pdf.

311 Corte Interamericana de Derechos Humanos, Caso de los Trabajadores Cesados del Congreso, Aguado-Alfaro et al. vs. Perú, (Sentencia del 24 de noviembre del 2006), http://www.corteidh.or.cr/docs/casos/articulos/seriec_158_ing.pdf.

312 Corte Interamericana de Derechos Humanos, Caso de Almonacid-Arellano et al vs. Chile, (Sentencia del 26 de septiembre de 2006), http://www.corteidh.or.cr/docs/casos/articulos/seriec_154_ing.pdf.

Convención. Este deber general del Estado Parte implica que las medidas de derecho interno han de ser efectivas (principio del effet utile), para lo cual el Estado debe adaptar su actuación a la normativa de protección de la Convención.[313]

En Argentina,[314] Colombia,[315] Chile,[316] México,[317] y Paraguay,[318] los tratados de derechos humanos ratificados por el Estado presentan las mismas características vinculantes que la constitución del país, y son jurídicamente exigibles en las cortes nacionales. Por ejemplo, la Suprema Corte mexicana reconoció que las autoridades y el ordenamiento jurídico mexicano deben respetar tanto las fuentes de derechos humanos constitucionales como las internacionales. No existe una relación jerárquica entre ellas; las dos fuentes de derechos humanos son igualmente importantes. Juntas representan un "parámetro de regularidad constitucional".[319] Cuando existe un conflicto entre estas, se entiende que, de acuerdo con el principio pro persona, se prefiere la norma jurídica más favorable para el individuo.[320]

En Colombia, la Corte Constitucional afirmó que los tratados internacionales de derechos humanos y el derecho humanitario internacional, junto con la constitución forman el "bloque constitucional", en el que juntos proporcionan la fuente para la normativa de los derechos humanos.[321] La Corte Constitucional de Colombia también admite declaraciones

313 Corte Interamericana de Derechos Humanos, Sentencia de Yatama vs. Nicaragua, (Excepciones Preliminares, Fondo, Reparaciones y Costas, 23 de junio de 2005), pár. 170, http://www.corteidh.or.cr/docs/casos/articulos/seriec_127_ing.pdf.

314 Corte Suprema de Argentina, Ekmekdjian, Miguel Ángel vs. Sofovich, Gerardo et al., 7 de julio de 1992. Para un análisis pormenorizado, lea a Verónica Ferrari y Daniela Schnidrig, Vigilancia Estatal de las Comunicaciones y la Protección de los Derechos Fundamentales en Argentina, (Electronic Frontier Foundation & Centro de Estudios en Libertad de Expresión y Acceso a la Información, marzo de 2016), URL.

315 Constitución de Colombia. art. 93. Vea también Jaime Rodríguez vs. Iván Mejía Alvarez, sentencia T-1319 (Corte Constitucional, 7 de diciembre de 2001), http://www.corteconstitucional.gov.co/relatoria/2001/t-1319-01.htm

316 Constitución de Chile, art. V y VI.

317 Constitución de México, art. I. La Constitución de México establece un principio pro persona, por el cual las disposiciones deben interpretarse de manera que favorezca a las personas y los derechos humanos. La Suprema Corte también reconoce las fuentes constitucionales e internacionales de la normativa de derechos humanos como componentes del mismo catálogo, el cual debe ser respetado por la autoridad y el ordenamiento jurídico mexicano (Suprema Corte. Sesión Plenaria. Contradicción de Tesis 293/2011).

318 Constitución de Paraguay, art. CXXXVII y CXLV.

319 Para una investigación pormenorizada, lea a Luis Fernando García, México: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México, Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales, (2016).

320 Luis Fernando García, México: Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México, Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales, (2016).

321 "[El] bloque de constitucionalidad tiene tres efectos jurídicos trascendentales: 1) los tratados de derechos humanos prevalecen sobre la legislación interna; 2) los tratados de derechos humanos pueden ser considerados como parámetros de constitucionalidad concurrentes con

realizadas por organismos internacionales como la Comisión Interamericana de Derechos Humanos, la Corte Interamericana de Derechos Humanos, y el Consejo de Derechos Humanos de la ONU como influencia para la interpretación de la legislación interna.[322] La Corte también le concede poder normativo a otros documentos internacionales además de los tratados, como a los principios internacionales. Ocasionalmente, la Corte utiliza documentos redactados por expertos, ya que se consideran importantes en la interpretación de la normativa internacional de derechos humanos.[323]

En Perú, los tratados de derechos humanos tienen que estar aprobados por el Congreso antes de que el Presidente de la República pueda ratificar.[324] Las normas relacionadas con las libertades y derechos reconocidos en la Constitución peruana se interpretan de conformidad con la Declaración Universal de los Derechos Humanos y otros tratados internacionales ratificados por Perú. La Constitución de este país también señala que en casos en que se presenten dudas o conflictos entre las leyes penales, el juez debe aplicar la ley que sea más favorable para el acusado.[325]

La Corte Constitucional de Guatemala también adhiere a esta doctrina de "bloque constitucional".[326] Las Constituciones de Guatemala y Perú dejan en claro que los derechos humanos consagrados en los tratados internacionales poseen una condición constitucional, incluso cuando no estén especificados en la constitución.

---

las normas constitucionales nacionales, por lo que un conflicto entre un tratado de derechos humanos y una ley interna puede derivar en una declaratoria de inconstitucionalidad; y 3) los derechos internacionalmente protegidos por los tratados de derechos humanos pueden ser invocados a través de las acciones nacionales destinadas a tutelar derechos constitucionales". Gongora Mera y Manuel Eduardo. La difusión del bloque de constitucionalidad en la jurisprudencia latinoamericana y su potencial en la construcción del ius constituionale commune latinoamericano, (Instituto de Investigaciones Jurídicas, Instituto Max Planck de Derecho Público Comparado y Derecho Internacional, 2014), http://www.corteidh.or.cr/tablas/r31277.pdf

322 Para un análisis completo sobre la doctrina del bloque constitucional, lea a Molina Carlos Ernesto, Acción parcial de inconstitucionalidad contra el artículo 19 del Código Sustantivo del Trabajo, Sentencia C-401, (Corte Constitucional, 14 de abril 2005), http://www.corteconstitucional.gov.co/RELATORIA/2005/C-401-05.htm y Rodrigo Uprimny Yepes, Bloque Constitucional, Derechos Humanos y Proceso (Escuela judicial Lara Bonilla, Consejo Superior de la Judicatura, Bogotá, 2006).

323 Para un análisis pormenorizado, lea a Camilo Rivera, Juan y Katitza Rodríguez, Colombia: Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales, Electronic Frontier Foundation (2016).

324 Constitución de Perú, art. LVI.

325 Constitución de Perú, art. CXXXIX, sección 9.

326 Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos humanos? Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos Peri, Luciana (coord.), (San José, C.R.: Fundación Acceso, 2015), 133.

Los tratados, acuerdos, y documentos de derechos humanos ratificados por Nicaragua y aprobados mediante acto legislativo se consideran legislación interna, y se aplican dentro y fuera de Nicaragua después de entrar en vigencia de manera internacional.[327]

Muchos países poseen cláusulas de preeminencia mediante las cuales un tratado prevalecerá en el momento en que se encuentre en conflicto con un estatuto nacional. Entre estos países se encuentran Colombia, Guatemala, y Honduras.[328] El Salvador tiene una manera similar de lidiar con los conflictos entre tratados y leyes nacionales, pero prioriza las disposiciones constitucionales cuando estas entran en conflicto con los tratados.[329]

327 Constitución de Nicaragua, art. CXXXVIII, sección 2.

328 Constitución de Guatemala, art. XLVI. Constitución de Honduras, art. XVIII.

329 Constitución de El Salvador, art. CXLIV-CXLIX. Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos humanos? Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos Peri, Luciana (coord.), (San José, C.R.: Fundación Acceso, 2015), LXXIV -LXXV.