Brasil

¿Cuál es el marco legal que protege la privacidad en Brasil? ¿Mis derechos están protegidos frente a la vigilancia estatal de las comunicaciones?

LIMITACIONES GENERALES A LA VIGILANCIA ESTATAL DE LAS COMUNICACIONES EN BRASIL	
DERECHOS	La Constitución Federal protege la libertad de expresión, la privacidad y la confidencialidad de las comunicaciones (artículo 5, apartados IX, X y XI).
	Las leyes nº 9.472/97 (artículos 3, V y IX, y 72) y nº 12.965/14 (artículo 7) garantizan el derecho de confidencialidad de las comunicaciones y el de privacidad en el uso de teléfonos e Internet.
	No existe un examen de limitaciones permisibles al derecho a la privacidad que hayan sido aplicados de manera uniforme en la jurisprudencia y el ámbito legal académico para evaluar las bases constitucionales de las limitaciones a tales derechos.
	El artículo 5, inciso 2 de la Constitución Federal establece que los derechos y garantías establecidos en ella no excluyen otros derechos que se originan del sistema y los principios reconocidos por la Constitución u otros tratados internacionales a los cuales Brasil suscribe. Sin embargo, los únicos tratados sobre derechos humanos que se consideran parte del bloque de constitucionalidad son aquellos que fueron aprobados por el Congreso, con el mismo procedimiento por el cual se reforma la Constitución, de acuerdo con lo dispuesto en el artículo 5, inciso 3.
RECURSOS	En el caso de la violación de los derechos, un individuo puede interponer un recurso de Habeas Corpus o *mandado de segurança* (similar a la solicitud de orden judicial), según lo contempla la Constitución (artículo 5, LXVIII y LXIX), o interponer una demanda bajo el proceso judicial ordinario.
GARANTÍAS	La Constitución Federal garantiza el debido proceso de la ley, sistema acusatorio, derecho a la defensa integral y presunción de inocencia (artículo, LIV, LV y LVII). El Código Procesal Penal exige a las cortes que se atengan a los principios de idoneidad, necesidad y proporcionalidad al momento de ordenar la recolección de evidencia (artículo 156). Lo mismo sucede con las reglas sobre las mociones que solicitan medidas cautelares sobre la presentación de evidencia (artículo 282). Las notificaciones de citación deben ser entregadas a la parte afectada "excepto en casos de emergencia o en casos en que exista la posibilidad de que la entrega pueda poner en riesgo la efectividad de la investigación" (artículo 282, inciso 3).
	Según la Constitución Federal (artículo 5, LVI) y el Código Procesal Penal (artículo 157), la evidencia obtenida a través de medios ilegales es inadmisible y no tiene validez.
SANCIONES	El artículo 10 de Ley nº 9.296/96 penaliza la interceptación ilegal y la violación del secreto judicial. Sanción: encarcelamiento de 2 a 4 años y multa.
	El artículo 156-A del Código Penal penaliza la violación de un dispositivo de tecnología de información con la intención de malversar datos. Sanción: encarcelamiento de 3 meses a 1 año y multa. Si la acción resulta en el acceso al contenido de información privada, la pena se aumenta de 6 meses a 2 años, y multa.

¿Cuál es el marco legal para interceptar comunicaciones en Brasil?

VIGILANCIA ESTATAL DE LAS COMUNICACIONES EN BRASIL			
Propósito / Autoridad	**Normativas en Telecomunicaciones (ANATEL)**	**Aplicación de la ley (Policía, Ministerio Público, Cortes y CPIs)**	**Inteligencia (Sisbin)**
OBLIGACIONES DE RETENCIÓN DE DATOS	Las resoluciones de ANATEL *(Resoluções)* nº 426/05, 477/07 y 614/13 exigen a los proveedores de servicios la retención de los metadatos concernientes a los servicios de líneas fijas y de telefonía celular por al menos 5 años y aquellos relacionados con las conexiones de Internet por al menos un año.	La Ley nº 12.850/13 (artículo 17) ordena que las compañías de telefonía fija y celular retengan "la identificación de registros de números telefónicos de origen y destino de terminales de conexión telefónica" por 5 años. La Ley nº 12.965/14 (artículos 13 y 15) ordena que proveedores de conexión específicos retengan los registros de conexión a Internet por 1 año y que los proveedores de aplicaciones con fines de lucro retengan los registros de acceso a las aplicaciones por 6 meses.	No existe obligación específica de retención con propósitos de inteligencia.
ACCESO A DATOS RETENIDOS (información de cuenta y metadatos)	En el desarrollo de sus deberes de supervisión (artículo 8, Ley nº 9472/97), la ANATEL puede acceder a documentos de facturación, que contienen la información de cuenta y el registro de llamadas, por medio de una solicitud hacia los proveedores de servicios. Actualmente, existe la infraestructura necesaria que permite el acceso en línea, directo e ilimitado, según lo estipula el artículo 38, *Resolução* nº 596/12. La Secretaría de Ingresos Federales de Brasil también puede solicitar acceso a los documentos de facturación (artículo 11, Ley nº 8.218/91).	De acuerdo con las Leyes nº 9.613/98 (artículo 17-B) y 12.850/13 (artículo 15), el acceso a la información de la cuenta de usuarios de teléfonos puede ocurrir simplemente con una solicitud a los proveedores de servicios por parte de las autoridades policiales o de los miembros del Ministerio Público. El acceso a registros de llamadas y otros metadatos generados por el uso del teléfono (por ejemplo, registros de ubicación) no posee ninguna norma legal específica: tiene lugar mediante una orden judicial con el fin de presentar evidencia. Según el *Mandado de Segurança* 23452/RJ, resuelto por la Corte Suprema Federal, el acceso a los registros de llamadas puede ser ordenado con la solicitud de las CPIs. Según la Ley nº 12.965/14, el acceso a la información de cuenta de los subscriptores de proveedores de Internet y de los usuarios de aplicaciones de Internet puede ocurrir cuando las autoridades con la jurisdicción correspondiente lo soliciten (artículo 10, inciso 3). En el caso de la conexión a Internet y el acceso a los registros de las aplicaciones, debe mediar una orden judicial cuando haya indicios fundamentados de infracciones, ya que los registros pueden ser relevantes para las investigaciones o hallazgos; debe delimitarse un periodo de tiempo específico (artículo 22).	La ABIN no tiene la facultad de solicitar ni de exigir datos. No obstante, es posible hacer que las agencias del Sisbin cooperen con tal fin (artículos 6, V y 6-A del Decreto nº 4.376/02).

ACCESO A REGISTROS DE COMUNICACIONES ALMACENADAS (contenido)	Las resoluciones de la ANATEL *(Resoluções)* permiten acceder a las grabaciones de las llamadas hechas a los servicios de atención al cliente de los proveedores de telecomunicaciones.	La Ley 12.965/14 permite acceder a comunicaciones privadas realizadas a través de aplicaciones de Internet mediante orden judicial (artículo 7, III). Conforme al *Recurso Extraordinário* 418.416-8/SC, resuelto por la Corte Suprema Federal, una orden de allanamiento e incautación admite el acceso a los datos contenidos en computadoras.	La ABIN no tiene la facultad de solicitar ni de exigir datos. No obstante, es posible hacer que las agencias del Sisbin cooperen con tal fin (artículos 6, V y 6-A del Decreto nº 4.376/02).
INTERCEPTACIÓN	La ANATEL no posee la prerrogativa para imponer ni autorizar interceptaciones.	De acuerdo con la Ley 9.296/96, la interceptación de comunicaciones telefónicas y de sistemas de tecnologías de la información puede tener lugar mediante orden judicial, ya sea por la iniciativa de la corte o por solicitud de las autoridades policiales o miembros del Ministerio Público, cuando exista una sospecha fundada de que el responsable o cómplice ha cometido un crimen, sancionado con encarcelamiento, o cuando no haya disponibilidad de otros medios para presentar evidencia (artículos 1 y 2). La Ley nº 12.965/14 permite la interceptación del flujo de comunicación a través de Internet de acuerdo con la Ley nº 9.296/96. Las resoluciones del Consejo Nacional de la Judicatura y del Consejo Nacional del Ministerio Público (Resoluções) establecen criterios que se deben seguir para las solicitudes y decisiones.	La ABIN no posee la prerrogativa para imponer o solicitar interceptaciones. La Ley nº 9.296/96 no le otorga a la ABIN tal facultad. No obstante, es posible hacer que las agencias del Sisbin cooperen con tal fin (artículos 6, V y 6-A del Decreto 4.376/02).

¿Quiénes y cómo pueden interceptar mis comunicaciones?

FUNCIONES INSTITUCIONALES Y SUS FACULTADES: AUTORIDADES RELACIONADAS CON PRÁCTICAS DE VIGILANCIA	
ANATEL	Creada bajo la Ley nº 9.472/97, ANATEL es la agencia reguladora a cargo de organizar la operación de la industria de las telecomunicaciones y de controlar la provisión de servicios relacionados (artículo 8). Tiene la potestad de aprobar normas (*resoluções*) (artículo 19).
	La agencia desempeña sus tareas al aprobar normas (*resoluções*) para mandar retención de datos, obligaciones para la identificación de los usuarios, y disposiciones acerca de la habilitación de fondos para la vigilancia, además de establecer sus propias prerrogativas para el acceso a los datos retenidos.
SECRETARÍA DE INGRESOS FEDERALES DE BRASIL	Agencia del Ministerio de Finanzas a cargo de administrar los impuestos al comercio nacional e internacional a través de la gestión y la aplicación de recolección, control e investigación, así como también a través del compromiso de cooperación internacional en materia de impuestos y aduana (artículo 15, Decreto nº 7.482/11). Tiene acceso a los documentos fiscales de proveedores de servicios de telecomunicaciones.
AUTORIDADES POLICIALES	Agencias encargadas de hacer cumplir la ley. Según la Constitución Federal (artículo 144), la Policía Civil Estatal y la Policía Federal conforman la Policía Judicial. Según el Código Procesal Penal, la Policía Judicial se encuentra a cargo de investigar infracciones penales e identificar a la persona responsable (artículo 4), por medio de procedimientos que son, por naturaleza, investigativos. La Fiscalía General controla los procedimientos de manera externa (artículo 129, VII, CF).
	El Código Procesal Penal establece que, tan pronto como la autoridad policial tome conocimiento de una infracción penal, esta deberá recolectar toda la evidencia que sea de utilidad para la investigación del caso (artículo 6, III). La Ley nº 12.830/13 determina que, durante una investigación penal, el Jefe de la Policía (*Delegado*) estará a cargo de solicitar la presentación de

	evidencia, información y datos que sean de interés para la investigación penal (artículo 2, inciso 2).
LA FISCALÍA GENERAL	De acuerdo con la Constitución Federal, la Fiscalía General es la entidad independiente del Estado dedicada a la protección del orden jurídico, el régimen democrático y los derechos de las personas (artículo 127). Los deberes de la Fiscalía incluyen presentar acciones colectivas, diligenciar notificaciones de procedimientos administrativos en su jurisdicción, solicitar información y documentos que las respalden, y ordenar investigaciones y pesquisas policiales (artículo 129).
	La ley complementaria nº 75/93 le otorga a la Fiscalía General la facultad de exigir información y documentos de entidades privadas y de realizar inspecciones e investigaciones dentro del alcance de sus deberes (artículo 8, IV y V); esto también se aplica, con carácter subsidiario, al Ministerio Público del Estado según lo establecido por el artículo 80 de la Ley nº 8.625/93. Esta ley también concede la facultad de exigir información a miembros del Ministerio Público (artículo 26, III).
AUTORIDADES JUDICIALES	Los Tribunales pueden, de manera oficial, ordenar la presentación y la entrega de evidencia según lo disponen el artículo 130 del Código Procesal Civil y el artículo 156 del Código Procesal Penal. Los Tribunales deciden sobre las solicitudes presentadas por las autoridades policiales y el Ministerio Público para la presentación de evidencia en investigaciones y casos penales cuando estén implicados los derechos protegidos por la Constitución, como la violación de información confidencial.
CPIs	Las Comisiones Parlamentarias de Investigación (CPIs) se crean temporalmente dentro del Poder Legislativo para averiguar sobre un hecho determinado; tienen los "poderes de investigación propios de las autoridades judiciales" según lo indica el artículo 58, inciso 3 de la Constitución Federal. Se les permite penetrar la confidencialidad de los datos almacenados sin la necesidad de que medie una orden judicial.
ABIN y SISBIN	De acuerdo con la Ley nº 9.833/99, la ABIN, la agencia de inteligencia central de Brasil y a la operadora del Sistema de Inteligencia de Brasil (SISBIN) les corresponde planear, organizar supervisar y controlar las actividades de inteligencia. Según el Decreto nº 4.376/02, además de la ABIN, el Sisbin también está compuesto por la Oficina del Jefe de Gabinete y la Oficina de Seguridad Institucional de la Presidencia de la República, aparte de un número de Ministerios y agencias relacionadas (como la Policía Federal, asociada al Ministerio de Justicia y la Secretaría de Ingresos Federales de Brasil, asociada al Ministerio de Finanzas). La supervisión externa se llevará a cabo por parte de una Comisión Conjunta del Congreso permanente, de acuerdo con el artículo 6 de la Ley nº 9833/99.
	La ABIN no posee las prerrogativas para exigir información, aunque puede ser capaz de acceder a los datos que están bajo la posesión de las áreas que conforman al SISBIN, según lo establece el Decreto nº 4.376/02 (artículo 6-A). No existen impedimentos para monitorear comunicaciones públicas.

Fuente: InternetLab

¿Cómo me entero si interceptan mis comunicaciones en Brásil?

No puedes saberlo. El Código de Procedimientos Penales (CPP) establece que un juez, a una solicitud de una Medida cautelar (por ejemplo, una orden de comparecencia u orden judicial) notificará a la parte afectada, "salvo en casos de emergencia o la posibilidad [de que el hecho de notificar podrá] comprometer la eficacia de la medida "(artículo 282, inciso 3). Mientras se llevan a cabo investigaciones criminales, se aplica esta excepción.

Cuando los casos criminales son llevados a juicio en los tribunales, el acusado será citado por el juez cuando sea necesaria la producción o la admisión de pruebas (tales como las obtenidas de intercepciones y violaciones de la confidencialidad de datos) (art. 370, CPP), de modo que el acusado se enterará de que ha sido sujeto de vigilancia.

En lo que respecta a los intermediarios, la mayor parte de las solicitudes de datos y órdenes de escuchas telefónicas están acompañados por “órdenes mordaza” que prohíben a las compañías telefónicas y proveedores de servicios de Internet notificar a sus usuarios. Empero, a pesar de la ausencia de una prohibición legal de notificar a los usuarios en otras

circunstancias, las empresas no están activamente comprometidas en esta práctica.

¿Puede, legalmente, el gobierno brasileño acceder a nuestras computadoras? ¿Bajo cuales circunstancias? ¿Cuál es su autoridad legal?

No existe claridad sobre cuál es el escenario legal en el que se permite este tipo de acceso, ya que no existe regulación específica sobre el hackeo gubernamental en Brasil. Sin embargo, reportes de la prensa sugieren que las autoridades policiales brasileñas afirman tener autoridad para instalar software espía en virtud de la Ley de intercepciones, y que los tribunales han aceptado las solicitudes y permitido esta práctica. Mientras tanto, los académicos y grupos de la sociedad civil han argumentado que la práctica es ilegal en ausencia de una autoridad legal bien definida para llevar a cabo este tipo de acciones invasivas.

Aunque no existe claridad jurídica en cuanto si es permitido el uso de este software o no, lo que si es cierto es que las autoridades policiales brasileñas han adquirido y tienen interés en tecnologías de hacking. Por ejemplo, en julio de 2015, la empresa italiana Hacking Team - conocido por el desarrollo y venta de software espía y herramientas de vigilancia a gobiernos y en apoyar a las instituciones policiales y militares en el espionaje a ciudadanos de todo el mundo - fue hackeada. Los documentos internos filtrados fueron publicados en línea; los mismos contenían numerosas referencias a las agencias de inteligencia en Brasil, tanto civiles como militares, así como a las empresas brasileñas que parecen ser los socios locales de Hacking Team.

Entre los organismos mencionados en los archivos se encuentran: Agencia Brasileña de Inteligencia (ABIN), el Centro de Inteligencia del Ejército (CIE), Centro de Instrucción para la guerra cibernética (CIGE), Departamento de Policía de Río de Janeiro Civil (CINPOL y DRCI), Departamento de Policía Militar de Río de Janeiro, Departamento de Policía Civil de Sao Paulo, Departamento de Policía Militar de Sao Paulo, Departamento de Policía Civil del Distrito Federal, Departamento de Policía Militar del Distrito Federal, Ministerio de Justicia, y la Oficina del Fiscal General de la República.

Los documentos filtrados plantean preguntas acerca de un mercado creciente de la vigilancia en Brasil y subrayan la necesidad de un debate jurídico acerca del tipo de datos que pueden ser interceptados, teniendo en cuenta la evolución de las nuevas tecnologías de vigilancia.

¿Cuántas comunicaciones han sido interceptadas por el Estado brasileño?

Gracias a las disposiciones de la Resolución nº 59/08 emitida por el Consejo Nacional de Justicia, los jueces de las cortes penales de todo el país están obligados a informar al Inspector General del Consejo Nacional de Justicia sobre los datos relativos a las operaciones de interceptación telefónica, así como también sobre la interceptación de tecnología de la información y sistemas telemáticos a través del Sistema Nacional de Control de Interceptaciones (Sistema Nacional de Controle de Interceptações), el cual recibe las notificaciones entregadas a los proveedores de servicios, los procedimientos presentados y números telefónicos, telefonía sobre IP (VoIP) y los correos electrónicos bajo vigilancia.

Los números obtenidos por InternetLab mediante un pedido de FOIA muestran que, en promedio, 18.000 líneas telefónicas por cada mes son intervenidas en Brasil. Sin embargo, Brasil no tiene criterios ni estadísticas sobre las escuchas telefónicas como si poseen algunos otros países de la región, por lo que la comparación de Brasil con ellos no es muy útil. Sabemos que en 2013, Estados Unidos, cuya población es de 120 millones mayor a la de Brasil, autorizó 3.576 órdenes de escuchas telefónicas. No sabemos cuántas órdenes de escuchas telefónicas fueron autorizadas en Brasil, pero 13.309 nuevos procedimientos de interceptación penal fueron presentados en 2013 (este número incluye escuchas

telefónicas pero no está desagregado). A su vez, Alemania, un país con menos de la mitad de la población de Brasil, emitió 19.398 órdenes iniciales de interceptación (Erstanordnungen) en el 2013. En Brasil, se conoce que se enviaron 50.265 notificaciones de interceptación a las compañías de telecomunicaciones durante el mismo periodo de tiempo.

Las estadísticas con relación a la interceptación en Brasil del Sistema Nacional de Control de Interceptaciones merecen estudio aparte. Si son altas, esto puede sugerir que, por un lado, que la protección que - teóricamente - brinda la necesidad de una orden judicial y la descripción de requerimientos estrictos para tales procesos como lo establece la Ley de Interceptaciones Telefónicas no se aplican en la práctica. Por otro lado, también puede señalar deficiencias estructurales en las capacidades de investigación de las autoridades de aplicación de la ley, haciéndolas altamente dependientes de este método agresivo de recopilación de información.

¿Es legal el uso de cifrado en Brasil?

La respuesta corta es Si. De acuerdo a la constitución Brasileña, nadie puede obligar a hacer algo o dejarlo de hacer salvo mandato expreso de la ley. El uso del cifrado no está prohibido expresamente por la ley de Brasileña. Ergo su implementación es legal.

La respuesta más prudente, sin embargo, es que depende. La Agencia Nacional de Telecomunicaciones de Brasil (ANATEL) ha ordenado a los proveedores de servicios de telefonía fija el poseer los recursos tecnológicos y las instalaciones suficientes de violar el secreto de las telecomunicaciones dentro del ámbito de las órdenes judiciales y que los mismos proveedores deben asumir los costes financieros de mantener este tipo de tecnología (artículo 24, Resolución n. 426/05). La Ley de Interceptación de Brasil también obliga a los proveedores de telecomunicaciones a cooperar con la policía en los procedimientos de escuchas telefónicas autorizadas por la ley (art. 7, Ley n. 9.296 / 96). En la práctica, esto limita el uso del cifrado y tecnologías similares por esos actores.

Mientras que estas obligaciones (similares a "CALEA") no se extienden directamente a las aplicaciones de contenidos "Over The Top" que proporcionan servicios de comunicaciones digitales, la gran popularidad de las aplicaciones de mensajería cifrada en Brasil ha suscitado un intenso debate en torno a esta tecnología en Brasil. Para mas información: https://www.eff.org/deeplinks/2016/03/punished-for-paradox-brazils-facebook and http://www.internetlab.org.br/pt/tag/whatsapp/