Vigilancia estatal de las comunicaciones en Brasil y la protección de los derechos fundamentales

Dennys Antonialli
Jacqueline de Souza Abreu

Diciembre de 2015

ELECTRONIC FRONTIER FOUNDATION

INTERNET LAB

El presente reporte es parte del proyecto regional "Vigilancia y derechos humanos" llevado a cabo en ocho países de América Latina por la Electronic Frontier Foundation, una organización internacional sin fines de lucro que, desde 1990, defiende la libertad de expresión y la privacidad en el entorno digital.

InternetLab es una organización sin fines de lucro dedicada a la investigación del derecho y las políticas de Internet en Brasil.

Autores

Dennys Marcelo Antonialli / Doctor en Derecho Constitucional, graduado de la Universidad de São Paulo (Brasil), donde también obtuvo su diploma de Licenciado en Derecho (LL.B., 2008). Posee una Maestría en Ciencias del Derecho de la Facultad de Derecho de Stanford (J.S.M., 2011) y una Maestría en Derecho y Comercio de la Facultad de Derecho de la Bucerius/WHU-Otto Beisheim Facultad de Administración de Alemania (MLB, 2010). Dennys ha trabajado en el Departamento de Políticas de la Unión Americana de Libertades Civiles de California del Norte (ACLU/NC) en el equipo de tecnología y libertades civiles y se ha desempeñado como asesor jurídico de Timor-Leste Legal Education Project (Facultad de Derecho de Stanford/Asia Foundation). En el 2011, ganó el primer puesto en los premios Steven M. Block Civil Liberties por mejor trabajo escrito sobre libertades civiles en la Facultad de Derecho de Stanford y el primer puesto en los premios Marco Civil y Desarrollo de Internet de Brasil (Google/FGV-SP). En 2013, se desempeñó como investigador en el Instituto Alexander von Humboldt para Internet y la Sociedad (Berlín). En julio de 2014, Dennys asistió al Programa Doctoral de Verano en el Instituto de Internet de Oxford. Actualmente, es el coordinador del núcleo de Derecho, Internet y Sociedad de la Universidad de São Paulo (NDIS-USP) y director ejecutivo de InternetLab.

Jacqueline de Souza Abreu / Estudiante del Máster en Derecho en la Facultad de Derecho de la Universidad de California en Berkeley. Posee una Maestría en Derecho de la Universidad Ludwig-Maximilians de Munich (LMU) y una Licenciatura en Derecho otorgada por la Universidad de São Paulo (LL.B., 2014). Durante sus estudios de posgrado, Jacqueline recibió becas de la Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) y del Programa de Estímulo ao Ensino de Graduação (PEEG) para llevar a cabo investigaciones en las áreas de Filosofía y Jurisprudencia, y fue parte del núcleo de Derecho, Internet y Sociedad de la Universidad de São Paulo (NDIS-USP). Jacqueline participó en un intercambio académico con la LMU, momento en el que recibió una beca del Servicio Alemán de Intercambio Académico (DAAD). También se desempeñó como investigadora junior en la FGV DIREITO SP.

Colaboradores

Francisco Brito Cruz (InternetLab)
Joana Varon Ferraz (Oficina Antivigilância)
Katitza Rodríguez (EFF)
Larissa Ribeiro (Oficina Antivigilância)
Luiz Alberto Perin Filho (Artigo 19)
Mariana Giorgetti Valente (InternetLab)
Paula Martins (Artigo 19)
Seth David Schoen (EFF)

Tabla de contenidos

Propósitos y estándares

El objetivo de este reporte es presentar las leyes relevantes sobre la vigilancia estatal de las comunicaciones y sobre la protección de los derechos fundamentales en Brasil. Hemos identificado sus fortalezas y problemas principales, y hemos hecho recomendaciones basadas en los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones[1]. A los efectos de este reporte, el concepto de vigilancia estatal de comunicaciones abarca interceptación, monitoreo, revisión, uso, retención y preservación de la información que incluye, refleja o se origina de las comunicaciones pasadas, presentes o futuras de algún individuo.

1.
Escenario legislativo

En las siguientes páginas, unas tablas ilustrativas. La tabla 1 presenta el panorama general de las normas constitucionales y legales que imponen límites a la vigilancia estatal de las comunicaciones en Brasil. A su vez, la tabla 2 muestra las instituciones gubernamentales asociadas a las prácticas de vigilancia y explica sus funciones. La tabla 3 resume el alcance de la vigilancia de las comunicaciones por parte del gobierno brasileño y la información que se detallará más adelante en este reporte. La tabla 4 indica cómo las prácticas de vigilancia estatal pueden expandirse como resultado de la colaboración internacional en materia penal.

Tabla 1: Limitaciones generales a la vigilancia estatal de las comunicaciones en Brasil

Fuente: InternetLab

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.

Tabla 2: Funciones institucionales y sus facultades

Fuente: InternetLab

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 sí tiene permitido 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.

Tabla 3: Vigilancia estatal de las comunicaciones en Brasil

Fuente: InternetLab

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).

Tabla 4: Asistencia judicial internacional en materia penal

Fuente: BELOTTO, Ana Maria de Souza; MADRUGA, Antenor; TOSI, Mariana Tumbiolo, Dupla incriminação na cooperação jurídica internacional, en: Boletim IBCCRIM, nº 237, agosto de 2012, disponible en: http://www.ibccrim.org.br/boletim_artigo/4678-Dupla-incriminao-na-cooperao-jurdica-internacional Consultado: 31 de julio de 2015.

TRATADOS DE ASISTENCIA JUDICIAL RECÍPROCA EN MATERIA PENAL	
Brasil es parte de diferentes acuerdos internacionales que abordan la asistencia judicial recíproca. Tales acuerdos provocan un impacto en la vigilancia de las comunicaciones a tal punto que permiten asistencia en la obtención y presentación de evidencia. De acuerdo con el principio de doble incriminación, la cooperación solo puede tener lugar cuando la actividad a la que se refiere la solicitud sea considerada un crimen en ambas jurisdicciones.	
REQUIERE CUMPLIMIENTO DEL PRINCIPIO DE DOBLE INCRIMINACIÓN	Acuerdos bilaterales con China, Corea del Sur, Cuba, Francia y Portugal.
REQUIERE EXCEPCIONALMENTE EL CUMPLIMIENTO DEL PRINCIPIO DE DOBLE INCRIMINACIÓN	Acuerdos bilaterales con Colombia, Estados Unidos, Italia, México, Nigeria, Panamá, Perú, el Reino Unido, Suiza, Suriname y Ucrania, y acuerdos multilaterales entre el Mercosur y la Organización de los Estados Americanos (OEA).
NO REQUIERE CUMPLIMIENTO DEL PRINCIPIO DE DOBLE INCRIMINACIÓN	Acuerdos bilaterales con España y Canadá.

2.

Crítica: virtudes y problemas en las prácticas de la vigilancia estatal en Brasil

2.1 Debilidades constitucionales en la protección contra la vigilancia indebida

La Constitución Federal brasileña de 1988 incluye, en la lista de derechos fundamentales, al menos tres apartados que son relevantes para la limitación de la vigilancia estatal de las comunicaciones en Brasil. El apartado IV del artículo 5 protege la libertad positiva de comunicaciones ya que garantiza la libertad de expresión ("IV – es libre la manifestación del pensamiento, quedando prohibido el anonimato"). En cambio, los apartados X y XII del mismo artículo protegen la libertad negativa de las comunicaciones, es decir, la posibilidad de mantenerlas en secreto o, al menos, limitada a aquellos a las que van dirigidas, ya que esto define el derecho a la privacidad ("X – Son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación") y confidencialidad de las comunicaciones ("XII – Es inviolable el secreto de la correspondencia, de las comunicaciones telegráficas, de las informaciones y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en la hipótesis y en la forma que la ley establezca para fines de investigación criminal o instrucción penal").

Aunque la confidencialidad de las comunicaciones esté protegida por la Constitución Federal de Brasil, los problemas de interpretación ponen en riesgo la protección real que tales derechos poseen contra la vigilancia indebida de las comunicaciones por parte de las autoridades.

Controversias: ¿qué tipo de confidencialidad protegemos?

En primer lugar, se encuentra la disputa sobre cuál es el alcance de protección establecido por el poco claro apartado XII del artículo 5 ("XII – Es inviolable el secreto de la correspondencia, de las comunicaciones telegráficas, de las informaciones y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en la hipótesis y en la forma que la ley establezca para fines de investigación criminal o instrucción penal"). Este apartado contempla la protección de la confidencialidad de las comunicaciones, pero su interpretación es un desafío debido a la falta de acuerdo en la jurisprudencia y el ámbito legal jurídico que permita una determinación constitucional clara para restringir los

derechos fundamentales; como consecuencia, tales determinaciones se realizan, en definitiva, caso por caso.

En general, las discusiones sobre la interpretación del apartado XII tienen dos facetas: (i) existe desacuerdo en lo que respecta a si la protección de este derecho fundamental va dirigida a la información trasmitida a través de los medios mencionados (correspondencia, mensajes telegráficos, datos, y llamadas telefónicas) o *comunicación*, es decir, el flujo de dicha información mientras es trasmitida; (ii) existe desacuerdo sobre qué categorías de las cuatro que fueron mencionadas están incluidas en la excepción que permite la violación de la confidencialidad[2] ("salvo, en el último caso"). Los académicos[3] son de la opinión, respaldada por una decisión de la Corte Suprema Federal,[4] de que la protección de la que se habla en el apartado XII del artículo 5 no hace referencia a la información trasmitida por medio de correspondencia, mensajes telegráficos, datos y llamadas telefónicas en sí, sino que se refiere a la comunicación, al flujo de estas a medida de que ocurren, y solamente la confidencialidad de las comunicaciones telefónicas, mientras están en proceso, pueden ser intervenidas para investigaciones y procesos penales; esta posibilidad no aplicaría al flujo de datos, mensajes telegráficos o cartas.

Gran parte de esta disputa trata de identificar un aspecto fundamental de protección *absoluta* en el artículo 5, apartado XII, en el que cualquier restricción sería inconstitucional: según lo estipulado anteriormente, la correspondencia, mientras está en tránsito, es absolutamente inviolable. Aunque muchos académicos del ámbito jurídico defienden esa postura, esta no se refleja en la jurisprudencia, la cual ya ha aceptado la "violación" de la confidencialidad del flujo de las comunicaciones de todo tipo, siempre y cuando sea "proporcional", cuando esté basada en un derecho fundamental o en el interés público.[5]

Adicionalmente, su interpretación limitada sobre que solo los flujos de información serían protegidos por el artículo 5, apartado XII, no sería suficiente para proteger el contenido de la información que ha sido almacenada, registrada o grabada, o incluso el contenido de la información sobre las circunstancias bajo las cuales las comunicaciones ocurren (metadatos). Esta interpretación también entra en tensión con la de la Corte Interamericana de Derechos Humanos en el Caso de Escher et. al. vs. Brasil (el cual se explicará con más detalle en la sección 2.5 de este reporte).

Clasificación de la privacidad: ¿información de cuenta < metadatos < contenido?

Incluso si la jurisprudencia y el ámbito legal académico brasileño consideran que solo el flujo de las comunicaciones es el sujeto de la protección que brinda el apartado XII del artículo 5, el derecho a la privacidad, contemplado de manera general en el apartado X del mismo artículo tiene en cuenta la protección de las comunicaciones en un sentido más amplio,[6] es decir, no solo el contenido de las comunicaciones sino también la información relacionada

con las circunstancias en las que tuvieron lugar y entre quiénes ocurrieron (esto se puede revelar a través de la información de cuenta [7] y metadatos[8]).

Como veremos a continuación, la legislación y jurisprudencia ordinarias brindan diferentes niveles de protección a estas distintas categorías de información, es decir, la información de cuenta, metadatos, y el contenido mismo de las comunicaciones. Esto significa que el grado de privacidad que se le da a la información depende de la naturaleza de esta. Sin embargo, estas distinciones ya no son apropiadas para medir el grado de intrusión que tiene la vigilancia de las comunicaciones sobre la vida privada de las personas y sus asociaciones. Tal como lo explican los estudiosos del derecho y expertos en privacidad de más de 70 países en los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,[9] se ha acordado desde hace tiempo que el contenido de las comunicaciones merece protección sustancial en la ley, debido a su capacidad de revelar información sensible, pero con el avance de la tecnología, queda claro que los metadatos y otras formas de datos que no están relacionados con el contenido pueden revelar incluso más información sobre una persona que el contenido propiamente dicho, y es por esto por lo que merece una protección análoga.[10]

No obstante, la legislación brasileña no proporciona ese nivel de protección a los datos que no están relacionados con el contenido de las comunicaciones. Por ejemplo, cambios recientes en la legislación han brindado menos protección para la información de cuenta, debido a que es considerada como información privada menos sensible. En términos prácticos, estos cambios jurídicos se llevaron a cabo para facilitar a las autoridades la obtención de tal información con solo solicitarla, sin la necesidad de que medie una orden judicial.[11] Esta disposición puede ser parcialmente considerada como una consecuencia inapropiada de la "prohibición constitucional de anonimato" brasileña, establecida en el apartado IV del artículo 5. Este, aunque debería aplicar solo a los casos de libertad de pensamiento, se usa de manera inadecuada para justificar la necesidad del acceso a dichos datos para identificar a posibles delincuentes en cualquier contexto.

La violación de la confidencialidad de los metadatos recibió un tratamiento legal que varía dependiendo de si se trata de datos telefónicos o de Internet. Generalmente, basta con una orden judicial. La interceptación, es decir, el acceso al contenido de las comunicaciones, requiere que se cumpla con los propósitos constitucionales y con los requerimientos legales específicos, los cuales deben ser garantizados mediante órdenes judiciales.

Otros pueden sostener que el apartado XII del artículo 5 protege únicamente el flujo de las comunicaciones y asumir que la información de cuenta y los metadatos son menos importantes para la privacidad. Esta postura no da cuenta del rol central que cumplen la información de la cuenta y los metadatos en la identificación de usuarios y en la interferencia hacia la información con respecto a sus intereses, contactos, y actividades. Como

consecuencia, se debilitan los límites impuestos a la vigilancia estatal de las comunicaciones en Brasil por los derechos fundamentales.

A nivel internacional, esta opinión también va en contra de las conclusiones del "Reporte anual del 2014 de la Oficina del Alto Comisionado para los Derechos Humanos de la ONU", el cual observa que "se ha sugerido que la interceptación o la recopilación de datos acerca de una comunicación, en contraposición al contenido de la comunicación, no constituyen en sí mismas una injerencia en la vida privada. Desde la perspectiva del derecho a la privacidad, esta distinción no es convincente. La agregación de la información comúnmente conocida como 'metadatos' puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada". [12]

2.2 ANATEL: vigilancia real "accidental"

En su jurisdicción para aprobar disposiciones normativas (artículo 19 de la Ley nº 9.472/97), que son *resoluções,* y en el desarrollo de sus deberes de agencia reguladora de telecomunicaciones, la *Agência Nacional de Telecomunicações* (ANATEL) regula y monitorea el suministro de servicios y hace respetar los derechos de los usuarios, pero no sin crear antes un potencial importante de vigilancia. La ausencia de precisión y claridad de las resoluciones de la ANATEL, así como también la falta de transparencia sobre la manera en la que se aplican, expone a los usuarios de los servicios de telecomunicaciones a la vigilancia estatal ilegal.

Deberes de los proveedores de servicios de telecomunicaciones

La *Resolução* nº 426/05 – *Regulamento do Serviço Telefônico Fixo Comutado* [Normativa del Servicio de Telefonía Fija Conmutada] exige, en el artículo 22, que "todos los datos relacionados con la provisión de servicios, incluyendo los registros telefónicos" sean retenidos por los proveedores de servicios de telefonía fija (tales como Vivo y NET) "por un lapso de al menos cinco años", sin precisar qué datos están incluidos, o por quiénes pueden ser utilizados, ni con qué propósitos. No existen normas de seguridad específicas en relación con el almacenamiento de estos datos: el artículo 23 únicamente establece la responsabilidad que tienen los proveedores de proteger la confidencialidad de los datos. El artículo 24 ordena a los proveedores de servicios de telefonía fija tener los recursos y la infraestructura tecnológica necesarios para violar la confidencialidad de las telecomunicaciones en el caso de que medie una orden judicial. También les exige a los proveedores correr con los gastos de mantenimiento de tales tecnologías.

La *Resolução* nº 477/07 – *Regulamento sobre* S*erviço Móvel Pessoal* [Normativa del Servicio Móvil Personal] establece asimismo, en el artículo 10, que los proveedores de

telefonía móvil (tales como Vivo, Claro, Tim y Oi) deben mantener, por un lapso mínimo de 5 años, "a disposición de la ANATEL y otras partes interesadas, los documentos de facturación (*documentos de natureza fiscal*), que contengan datos sobre llamadas entrantes y salientes, fecha, hora, duración, y precio, así como también la información de cuenta de los subscriptores, de acuerdo con lo dispuesto en el artículo 11 de la Ley nº 8.218/91 [...]," la cual exige a las entidades legales retener y mantener los documentos fiscales/de facturación a disposición de la Secretaría de Ingresos Federales de Brasil, por un periodo de 5 años estipulado en la normativa tributaria como el plazo mínimo para presentar acciones ante la Corte (*prazo decadencial*). Los artículos 42 y 58 también establecen "un mínimo de datos personales" que las personas deben proveer para contratar un servicio de telefonía móvil (nombre, número del documento de identidad, y número de identificación fiscal). En la práctica, esto hace que el registro de un móvil dependa de un número de identificación fiscal, lo que compromete el uso anónimo.

Las razones acerca de la obligación a los servicios telefónicos de retener datos por cinco años y la justificación de los propósitos de las auditorías de facturación y supervisión llevada a cabo por la ANATEL están descritas en el artículo 10, XXII de la *Resolução* nº 477/07. No obstante, ambas normas (las obligaciones de retención de datos impuestas en la telefonía fija y móvil) han hecho que el almacenamiento de tales registros sea conveniente para los objetivos del Estado para llevar a cabo tareas de investigación y acusación. La Ley nº 12.850/13 [Legislación sobre organizaciones criminales], que exigía a las compañías telefónicas retener datos expresamente con ese fin, data del año 2013. Adicionalmente, las disposiciones de estas *resoluções* imponen obligaciones de retención de datos incluso para los servicios con planes de tarifa plana, en los que la duración de la llamada o el número al que se llama no altera el monto que el usuario debe pagar. Por eso, es razonable suponer que las normativas de la ANATEL relacionadas con la recolección de datos tienen propósitos que van más allá de aquellos asociados con sus responsabilidades.

La *Resolução* nº 614/13 – *Regulamento do Serviço de Comunicação Multimídia* [Normativa de Servicio de Comunicación Multimedia] exige, en el artículo 53, que los proveedores de servicios de conexión a Internet (tales como Vivo y NET) retengan los registros de conexión y los datos de cuenta de los subscriptores por al menos un año. El artículo 4, apartado XVII brinda la definición de registros de conexión (el conjunto de datos referidos a la fecha y hora del uso de una conexión a Internet, una dirección IP específica usada en la terminal de paquetes de datos entrantes y salientes, entre otros datos que permitan la identificación de la terminal de acceso utilizada). Este lapso de retención más corto en comparación con la obligación de retención de datos de los servicios telefónicos, así como también la descripción de los datos que deben ser retenidos, puede atribuirse al hecho de que esta norma se redactaba mientras tenían lugar las discusiones concernientes a la Ley nº 12.965/14 (*Marco Civil da Internet*) y a la publicidad relacionada con las decisiones internacionales en contra de la retención de datos, que recibió especial atención por parte de

la comunidad académica y la sociedad civil.

Acceso directo a datos

El acceso de la ANATEL a los documentos de facturación de los proveedores *(documentos de natureza fiscal)*, que, como hemos visto, contienen los datos de cuenta de los clientes, los registros de uso, y los precios de las llamadas, está generalmente disponible con propósitos de inspección cuando la agencia lo solicite.

Un artículo publicado en el diario *Folha de São Paulo en* el 2011[13] reveló que la agencia tenía la intención de contar con acceso directo y sistemático a tales datos a través de la construcción de una infraestructura que habilite a la ANATEL a tener acceso *online* ilimitado con el propósito de modernizar su facultad de supervisión. En ese momento, la agencia manifestó que el acceso a los registros telefónicos sólo tendría lugar con el permiso de los usuarios que soliciten la revelación de los registros,[14] y que el software por instalar solamente permitiría el acceso a los datos crudos de los proveedores, sin relación con la información de cuenta.[15]

El artículo 38 de la ANATEL *Resolução* nº 596/12 impuso a los proveedores de servicios telefónicos la obligación de entregar datos, permitir el acceso, y poner a disposición el acceso en línea a aplicaciones, sistemas, recursos tecnológicos, e instalaciones que ellos usan "para la recolección, procesamiento y entrega de los datos, información y otros elementos", lo que confirmó lo comunicado por el diario *Folha*. Los compromisos previos de la ANATEL sobre las limitaciones al acceso de los datos de los usuarios no se implementaron de manera expresa en esta *resolução*.

2.3. Secretaría de Ingresos Federales de Brasil: la vigilancia de las comunicaciones "entre líneas"

El artículo, XXII de la mencionada *Resolução* de la ANATEL (nº 477/07) muestra que el razonamiento que subyace a la obligación de retener información de cuenta y registros telefónicos por al menos cinco años está relacionado con el artículo 11 de la Ley nº 8.218/91, el cual exige a las entidades legales mantener los documentos de facturación a disposición de la Secretaría de Ingresos Federales de Brasil por el periodo de tiempo establecido en la normativa tributaria. Esto significa que no solo la ANATEL, sino que también la propia Secretaría de Ingresos Federales de Brasil puede, en el desarrollo de su gestión tributaria y responsabilidades de auditoría, obtener acceso a la información de las comunicaciones de los usuarios, mediante la solicitud de documentos de facturación que contienen tales datos (en el caso de teléfonos móviles, a los cuales aplica la *resolução* en cuestión, el mínimo de datos será el número al que se llama, la hora, fecha, duración y el precio asociados con esa cuenta o llamada).

Dado que la obligación de retener documentos de facturación se extiende a todas las entidades legales, las prerrogativas de la Secretaría de Ingresos Federales de Brasil tienen el potencial de llegar a cualquier usuario de telecomunicaciones de Brasil cuando tales documentos sean capaces de revelar información sobre el comportamiento de los usuarios, incluso utilizando solamente los metadatos y la información de la cuenta.

En julio de 2015, la *Oficina Antivigilância* destacó la realización de un acuerdo entre el Departamento de Seguridad Interior de Estados Unidos, la Oficina de Aduanas y Protección Fronteriza de Estados Unidos y el Ministerio de Finanzas de Brasil, a través de la Secretaría de Ingresos Federales de Brasil, de "reconocimiento mutuo" del programa estadounidense de "la Asociación de Aduanas-Comercio en contra del Terrorismo" y el programa brasileño "Operador Económico Autorizado" de la Secretaría de Ingresos Federales, el cual incluiría la transferencia de infraestructura de procesamiento de datos, y el desarrollo y uso de una tecnología de información en común.[16] Debido a que la Secretaría de Ingresos Federales de Brasil posee potencial acceso a la información detallada de los brasileños, esta cooperación puede resultar en la expansión de la vigilancia de las comunicaciones.

2.4. Vigilancia con y sin pesos y contrapesos: telefonía vs. Internet

Existen dos leyes federales recientes que han regulado la capacidad de la vigilancia de las comunicaciones por el Estado con el fin de hacer cumplir la ley*:* la firma de una nueva Ley de Organizaciones Criminales y del *Marco Civil da Internet*. El primero da lugar a preocupaciones serias sobre el abuso de los poderes de vigilancia, especialmente en la industria de la telefonía, mientras que el segundo —desarrollado en el contexto de debate público amplio y extensivo —crea y limita al mismo tiempo la vigilancia en Internet.

Ley de Organizaciones Criminales (Ley nº 12.850/13)

Obligación de retención de registros telefónicos

El artículo 17 de la Ley de Organizaciones Criminales establece que "las concesionarias de telefonía fija y móvil mantendrán, por cinco años, y a disposición de las autoridades mencionadas en el artículo 5 [el jefe de la Policía Civil y la Fiscalía General], los registros para identificar los números de terminales entrantes y salientes de llamadas internacionales, de larga distancia o locales". La existencia de esta obligación en la Ley de Organizaciones Criminales sugiere que está destinada para los fines legítimos de investigar organizaciones criminales, aunque lamentablemente esta ley no contenga ninguna disposición que restrinja el uso de los datos retenidos para la investigación de actividades de organizaciones criminales.

La inclusión de una obligación tan amplia en una ley tan específica puede haber encubierto el incremento del poder de la vigilancia estatal de las comunicaciones, más aún debido a que pasó casi desapercibida en los debates públicos y académicos, además de no haber pasado por el control de legalidad, necesidad y proporcionalidad, y no incluyó especificaciones detalladas sobre los datos por registrar, las entidades a las que aplica, las limitaciones de los accesos, las condiciones de uso ni las normas de seguridad de los datos. La constitucionalidad de esta disposición se impugnó mediante una demanda de inconstitucionalidad *(Ação Direta de Inconstitucionalidade* ADI 5063/DF), la cual está en espera de juicio y será desarrollada más abajo.

Prerrogativas de acceso a la información de cuenta

El artículo 15 de la Ley de Organizaciones Criminales establece que "el jefe de la policía civil y la Fiscalía General tendrán acceso, sin necesidad de que medie una orden judicial, solamente a la información de cuenta de la persona acusada que indique aptitudes personales, sus padres y la dirección retenida por las Cortes Electorales, *compañías telefónicas*, instituciones financieras, *proveedores de Internet* y administradores de tarjetas de crédito" (sin itálicas en el original). Esa disposición repite el lenguaje utilizado en el artículo 17-B de la Ley de Crímenes de Lavado de Dinero (Ley nº 9.613/99), la cual se agregó recientemente a través de la Ley nº 12.683/2012.

Es importante mencionar que las normas que renunciaban al requerimiento de obtener una orden judicial para acceder a tal información tienen su origen en una reforma legislativa reciente. Anteriormente, la posibilidad de violar la confidencialidad de la información de cuenta sin una orden judicial era una cuestión controvertida entre los académicos jurídicos y en la jurisprudencia. Esto era así debido a que, aunque el artículo 6, apartado III del Código Procesal Penal permita a las autoridades policiales "recopilar toda la evidencia relevante para clarificar los hechos y circunstancias" cuando se informe sobre la comisión de un crimen, y el artículo 8, apartado IV de la Ley Complementaria nº 75/93 permita a la Fiscalía General solicitar "información y documentos a entidades privadas" en el desarrollo de sus responsabilidades, lo cual aplica, con carácter subsidiario, a las entidades estatales (artículo 80 de la Ley nº 8.625/93), el acceso a dicha información fue rechazado por las compañías, al argumentar que la información estaría protegida por el artículo 5, apartado X de la Constitución Federal, y que por esa razón se necesita una orden judicial para la violación de la confidencialidad.[17]

Las disposiciones aprobadas recientemente cambiaron estas normas en respuesta a la presión de autoridades investigadoras sobre legislación específica que les conceda "acceso libre" —bajo mera solicitud— que haga más eficiente las investigaciones y procesos legales. Si bien las normativas sobre crimen organizado y lavado de dinero actualmente les permiten el acceso a esta información bajo solicitud, las autoridades mencionadas también están tratando de expandir su acceso a estos datos con otros propósitos, ya que la legislación no limitó de manera expresa los propósitos para los cuales estos datos pueden utilizarse.[18]

En la práctica, dichas autoridades utilizan estas disposiciones para apoyar las solicitudes de datos de los proveedores de servicios de telefonía; solo si la compañía se rehúsa a obedecer, se llevará el asunto a la Corte para su revisión.

¿También prerrogativas de acceso a registros telefónicos?

Desde la promulgación de la Ley de Organizaciones Criminales, las autoridades con la jurisdicción adecuada, especialmente los jefes de la policía civil, han solicitado registros telefónicos a las compañías de telefonía sin órdenes judiciales, basadas en la interpretación conjunta de los artículos 15, 17, y 21 de esta ley.

Según el artículo 15, "el jefe de la policía civil y la Fiscalía General tendrán acceso, sin necesidad de que medie una orden judicial, solamente a la información de cuenta de la persona acusada que indique aptitudes personales, sus padres y dirección" que retienen las compañías telefónicas. Sin embargo, el artículo 17 exige a las compañías de telefonía fija y móvil almacenar "los registros de identificación de los números de origen y destino de terminales de conexión telefónica" por cinco años "y dejarlas a disposición de las autoridades mencionadas en el artículo 15". A su vez, la cláusula principal del artículo 21 penaliza que las compañías se rehúsen o no cumplan con la entrega de "información de cuenta, registros, documentos e información que exija la Corte, la Fiscalía General o el jefe de la policía civil en el curso de una investigación o proceso penal", e impone sanciones que varían desde seis meses hasta dos años de prisión, y multa.

Como consecuencia, dichas autoridades han exigido no solo la información de cuenta sino también los registros telefónicos (e incluso algunos datos de ubicación), sin tener órdenes judiciales. Las solicitudes directas se realizan a las compañías, bajo amenaza de sanción por incumplimiento.

La *Ação Direta de Inconstitucionalidade* (ADI 5063/DF, a la que nos referimos más arriba), un recurso de constitucionalidad, se presentó en la Corte Suprema Federal por parte de una asociación de operadores móviles celulares, la *Associação Nacional de Operadoras Celulares* (ACEL), en busca de anular estos artículos, debido a que violan el derecho a la privacidad y el principio de legalidad, ya que la inexactitud de las normas da lugar a inseguridad jurídica.[19] Este recurso todavía está a la espera de juicio.

Marco Civil de Internet (Ley nº. 12.965/14)

Obligaciones de retención de datos

Con respecto a los registros de conexión, el artículo 13 del *Marco Civil da Internet* establece que "al proveer una conexión de Internet, el sistema proveedor independiente que corresponda (tales como Embratel, Oi, UOL Diveo y muchos otros, como algunas universidades) tiene el deber de almacenar los registros de conexión, en confidencialidad y en un ambiente seguro y controlado, por el periodo de un año, conforme a la normativa vigente". Los sujetos de esta obligación, los "administradores de sistema independientes", son, según el artículo 5, IV de la ley, un "individuo o entidad legal que se encarga de los bloques de direcciones IP y los sistemas de ruteo correspondientes, que están debidamente inscritos en la agencia nacional a cargo de registrar y distribuir las direcciones IP para todo el país", lo cual alcanza a los proveedores de acceso a Internet que cumplan con esta definición.[20]

Según el artículo 5, apartado VI, los registros de conexión conforman "el conjunto de datos concernientes a la fecha y hora de comienzo y fin de una conexión a Internet, su duración y la dirección IP usada por la terminal para enviar y recibir paquetes de datos". Debido al riesgo a la privacidad de los usuarios de Internet, el artículo 14 prohíbe a los proveedores retener los registros de acceso a las aplicaciones (es decir, a sitios y servicios online específicos).

A su vez, el artículo 15 del *Marco Civil da Internet* establece que "los proveedores de aplicaciones de Internet conformados como entidades legales e involucrados en los negocios de manera organizada y profesional y con fines de lucro, deberán mantener la confidencialidad de los registros de acceso a las aplicaciones de Internet, en un ámbito controlado y seguro, por seis (6) meses de acuerdo con la normativa vigente". Según el artículo 5 apartado VII, una aplicación es el "conjunto de funciones a las que se puede acceder por medio de una terminal conectada a Internet".

El sujeto de esta obligación no es el proveedor de la aplicación, sino aquellos que estén involucrados en tal actividad con capacidad comercial. No obstante, se les puede solicitar a los proveedores de aplicaciones no comerciales que retengan datos, mediante orden judicial, "siempre y cuando se refiera a registros concernientes a hechos específicos de un periodo de tiempo determinado", según lo dispone el inciso 1 del artículo 15. Los datos específicos que incluye la obligación general de retención de datos son, según lo definido en el artículo 5 apartado VIII, "el conjunto de información relacionada con la fecha, la hora y el uso de una aplicación de Internet en particular, en una dirección IP específica".

Con respecto a la obligación de retener los registros de conexión a Internet y el acceso a las aplicaciones en general, existen tres comentarios que son pertinentes. Primero, el inciso 2 del

artículo 13 y el inciso 2 del artículo 15 admiten la posibilidad de mociones, por medio de procedimientos cautelares, que extiendan los periodos de retención de datos para entidades específicas en situaciones específicas, y no hay ninguna norma con respecto al lapso máximo para tal extensión. Segundo, el inciso 4 del artículo 10 y las cláusulas principales de los artículos 13 y 15, hacen referencia a las medidas de seguridad para la retención y disponibilidad de los registros, mientras que el artículo 12 penaliza la violación de los mismos. Tercero, la normativa a la que se refieren los artículos 13 y 15, los cuales probablemente introducirán más especificaciones con respecto a aquellos responsables de retener los datos y tomar las medidas de seguridad, todavía no fue aprobada; sin embargo, ha pasado la instancia preliminar de indagación pública, habiendo recabado recomendaciones y debates, y está siendo estructurada. Se espera que mejore la protección contra la vigilancia indebida.

Prerrogativas de acceso a la información de cuenta

El artículo 10, inciso 3 del *Marco Civil da Internet* establece que la protección de datos personales y de comunicaciones privadas asegurados bajo la cláusula principal "no impide el acceso a la información de cuenta que indica identificación personal, padres y dirección, como lo contempla la ley, por parte de autoridades administrativas que tengan jurisdicción para la obtención de tal información". En lo que respecta a esta disposición, los miembros de la comunidad académica y la sociedad civil han sostenido que el Decreto reglamentario prescrito por el *Marco Civil da Internet* debería esclarecer los límites de dicho acceso para evitar abusos, e identificar expresamente las autoridades con jurisdicción pertinente, ya sea exigiendo que exista una relación cercana entre la autoridad solicitante y los motivos específicos de tal pedido, o bien evitando el acceso sin tener orden judicial y limitándolo a los términos de la Ley de Organizaciones Criminales y Lavado de Dinero.[21]

También se espera que el Decreto aborde el tema de las solicitudes de acceso a información de cuenta realizado mediante el uso de datos contenidos en los registros de acceso a aplicaciones (la obtención de la dirección IP y la hora), lo que, en principio, burlaría el requerimiento de orden judicial para violar la confidencialidad de los registros de conexión a Internet.[22]

Acceso a registros de conexión a Internet y acceso a aplicaciones

El artículo 10, inciso 3 del *Marco Civil da Internet* establece de manera específica que el acceso a los registros de conexión a Internet y el acceso a las aplicaciones dependerán de una orden judicial, protección que se refuerza en los artículos 13, inciso 5 y 15, inciso 3. A su vez, el artículo 22 limita los propósitos a la "producción de un conjunto de pruebas para casos civiles y penales", y estipula los requerimientos con los que la "parte interesada" debe cumplir para que se le otorgue una orden judicial: poseer indicios fundamentados de delincuencia; justificar la utilidad de los registros solicitados para los fines de la investigación o hallazgos; especificar los periodos a los que se refieren los registros.

Por último, el artículo 23 le encomienda a la Corte la tarea de "adoptar las medidas necesarias para garantizar la confidencialidad de la información recibida y la preservación de la privacidad del usuario, su vida privada, su honor e imagen, y puede ordenar que los casos se vean a puerta cerrada, inclusive con respecto a las mociones para la retención de registros".

Acceso a comunicaciones privadas almacenadas

La cuestión de la violación de la confidencialidad del contenido de comunicaciones electrónicas bajo la posesión de los proveedores de aplicaciones de Internet (tales como Google y Facebook) también está cubierta por el *Marco Civil da Internet*, en los artículos 7, III y 10 inciso 2, los cuales exigen que exista una orden judicial para este caso. Estas disposiciones, junto con el artículo 11, que exige el cumplimiento de la legislación brasileña por parte de los proveedores que recopilan, retienen o procesan datos, se incluyeron en el *Marco Civil da Internet* probablemente para construir los cimientos jurídicos para la solicitud de entrega de datos retenidos en el exterior.

Antes de la promulgación del *Marco Civil da Internet,* aparentemente era más difícil exigirles a los proveedores que entreguen dichos datos, ya que ellos podían fácilmente alegar que los datos estaban sujetos a la legislación extranjera, y pedir que se cumpla con los procesos legales internacionales específicos.[23] Como consecuencia, el inciso 2 del artículo 11 estableció de manera expresa que "las disposiciones de la cláusula principal aplican incluso cuando a las actividades las llevan a cabo entidades legales con sede en el exterior, siempre que provean servicios a los brasileños o al menos un miembro del mismo grupo económico brasileño que opere en Brasil." Aun cuando, por un lado, el *Marco Civil da Internet* estableció claramente la necesidad de una orden judicial para proteger algunas categorías de presentación de evidencia, por otro lado, expandió las capacidades de vigilancia de las comunicaciones del Estado brasileño.

Asimismo, la inclusión de dichas disposiciones en el *Marco Civil da Internet* no resolvió el asunto de jurisdicción, ya que los proveedores aún pueden impugnar la aplicación de la ley brasileña a datos retenidos en el exterior, lo que ha resultado en órdenes judiciales controvertidas y desproporcionadas. [24]

Expansión de la vigilancia en ausencia de legislación sobre comunicaciones telefónicas

La vigilancia telefónica con propósitos de aplicación de la ley está improvisada en la Ley de Organizaciones Criminales. No existe una Ley sistemática que regule las obligaciones de resguardo, las circunstancias en las que el acceso está permitido, ni los propósitos que se cumplen mediante el acceso. Es decir, no existe una “Declaración de Derechos en las Comunicaciones Telefónicas" que limite la vigilancia. En este contexto, se ha ignorado la aplicación del derecho internacional de los derechos humanos.

Por ejemplo, no existe una disposición que limite las violaciones de confidencialidad a los casos penales, y excluya los casos civiles, o acote los registros de llamadas (las llamadas recibidas y realizadas, la fecha, la hora y su duración) sobre los que apliquen las obligaciones de resguardo y que no aplique a los datos de ubicación (Estaciones de Base de Radiocomunicaciones, por ejemplo). En la práctica, el resultado es que la confidencialidad de *cualquier* metadato generado mediante un teléfono puede ser violado *cada vez que* así lo determine una Corte.

Un síntoma de lo mencionado es el caso resuelto por el Tribunal de Justicia de Rio Grande do Sul en julio de 2007 que permitió violar la confidencialidad de los datos de ubicación de un usuario de teléfono por el incumplimiento del pago de la pensión alimenticia bajo los registros del procedimiento para el cumplimiento de esta obligación. Se le ordenó al acusado pagar la pensión alimenticia e incumplió con la orden sin causas, por lo que se le emitió una orden de arresto. La identificación de localización no tuvo éxito en los muchos intentos que se hicieron. Teniendo esto en cuenta, para "proteger completamente a los niños y adolescentes", la Jueza de la Corte de Apelaciones permitió la "escucha telefónica" para recopilar datos sobre la ubicación del acusado, basándose en su número telefónico. [25]

Limitaciones a la vigilancia de Internet en el Marco Civil

El *Marco Civil da Internet*, por otro lado, está dando frutos con respecto a la limitación de la vigilancia indebida. En una sentencia de abril de 2015,[26] la Corte Federal de São Paulo invalidó una solicitud presentada por un oficial de la Policía Federal hacia la plataforma Twitter, en la que pedía "tantos datos como sea posible, tales como la dirección IP del acceso, las fechas de acceso, la identificación completa y la información de cuenta del usuario @EnkiEa666". La Policía Federal argumentó que el inciso 3 del artículo 10 del *Marco Civil da Internet* "permite a las autoridades administrativas solicitar información de cuenta y la Ley nº 12.830/2013 autoriza de manera explícita a los oficiales de policía, durante el curso de una investigación policial, solicitar datos e información relevantes para la investigación", como lo determina el artículo 2, inciso 2, de esa Ley.

En su sentencia, el juez federal reconoce que la solicitud presentada por la autoridad policial abarca no solo la información de cuenta del usuario, sino que también los registros de acceso a la aplicación e indica que "la ley [*Marco Civil da Internet*] permite a las autoridades administrativas competentes solicitar información sobre sus usuarios a los proveedores de Internet, siempre que esa información esté limitada a la información de cuenta, como la identificación personal, la información parental y la dirección. Por lo tanto, en mi opinión, la información relativa a los registros de conexión y de acceso a la aplicación de Internet, así como también los datos y el contenido de las comunicaciones privadas, está sujeta a una orden judicial como lo determina explícitamente el artículo 10, inciso 1 de la Ley nº 12.965/14."

Con respecto a la información de la cuenta, el juez aceptó lo clarificado por Twitter, sobre que no tenía información como el nombre completo del usuario, su dirección ni la información de sus padres. En cuanto a los registros de acceso a la aplicación, el juez concluyó que Twitter no tenía la obligación de poner a disposición estos datos debido a la falta de orden judicial que exija su divulgación.

2.5. Interceptación: vigilancia restringida en la teoría y extensiva en la práctica

Teoría: Leyes sobre Interceptación Telefónica y resoluciones (*Resoluções*) del Consejo Nacional de la Judicatura y del Consejo Nacional del Ministerio Público

La Ley nº 9.296/96 ("Ley de Interceptación Telefónica") regula este tipo de procedimiento típico de la vigilancia en Brasil. El artículo 1, párrafo único, de esta ley expande el alcance de la normativa a "la interceptación de las comunicaciones que transcurren vía tecnologías de información y medios telemáticos", incluyendo así las comunicaciones de datos que circulan por Internet, como los correos electrónicos. En la controversia sobre la interpretación correcta de la disposición constitucional que protege la confidencialidad de las comunicaciones, se impugnó su 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.[27]

No obstante, la *Ação Direta de Inconstitucionalidade* 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 lo 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 nº 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 (artículo 3). En vista de dichas disposiciones, está prohibida la interceptación solicitada por autoridades que no hayan sido designadas de manera expresa, como la *Agência Brasileira de Inteligência* (ABIN). El artículo 2 limita aun más la circunstancia bajo la cual la interceptación puede tener lugar: *no* se permitirá en los casos en los que no haya pruebas razonables de responsabilidad penal o conspiración en la comisión de un crimen; en el caso de que las pruebas puedan obtenerse por otros medios; o cuando el acto bajo investigación tenga pena menor a una sentencia de encarcelamiento del tipo "*detenção*" (común para los delitos menores).

El único párrafo del artículo 2 y los artículos 4 y 5, a su vez, aseguran que la interceptación solo ocurrirá si está debidamente justificada: una 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; la sentencia establecerá cómo deberá llevarse a cabo. El artículo 5 estipula que el periodo de interceptación no excederá los 15 días, sujeto a prórroga de la orden judicial: se dará "prórroga por un periodo de tiempo equivalente cuando sea necesario por razones probatorias". Aunque el artículo 5 podría admitir la interpretación de que el periodo máximo de tiempo de interceptación es 30 días, la jurisprudencia imperante[28] sostiene que una orden de interceptación puede ser prorrogada por *tanto como se requiera.* El artículo 7 concede a las autoridades policiales la facultad de solicitar a "los servicios y al personal especializado de servicios públicos" que lleven a cabo los procedimientos de interceptación. 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. Se considera un crimen a la interceptación ilícita, según lo dispone el artículo 10. En vista de lo anterior, se puede argumentar que, como regla general, la Ley de Interceptación Telefónica contiene disposiciones que tienen como objeto asegurar que la interceptación ocurra solamente en los casos en que el interés público justifique la restricción de la privacidad de las comunicaciones.

Una norma elaborada por el Consejo Nacional de Justicia (CNJ), *Resolução* nº 59/08, contempla de manera administrativa el procedimiento para solicitar la interceptación, establece los estándares para las resoluciones judiciales en la materia, define la manera en que se debe notificar a las compañías de interés, y hace responsables a los jueces de proteger la privacidad de la información interceptada. La *Resolução* nº 36/09 del Consejo Nacional del Ministerio Público (CNMP) contiene disposiciones similares en lo que respecta a las formas de solicitud y de realización de la interceptación.

El objetivo de dichas resoluciones, que llenan un vacío legislativo, es limitar las posibilidades de que ocurra un abuso cuando se emita una orden judicial, reducir los riesgos que pueden afectar la confidencialidad, y por lo tanto, el éxito de las investigaciones, e incrementar la seguridad de la información interceptada. Asimismo, también estipulan que los miembros de la Fiscalía General y los jueces deben informar mensualmente al Inspector General de la Fiscalía General (*Corregedoria-Geral do Ministério Público)* y al Inspector General del Consejo Nacional de Justicia (*Corregedoria Nacional da Justiça*), respectivamente, sobre el número de operaciones de interceptación en curso (artículo 10 del CNPJ *Resolução* nº 36/09 y artículo 18 del CNJ *Resolução* nº 59/08), a efectos estadísticos.

Práctica: uso impreciso de interceptaciones

Caso de Escher et al. vs. Brasil – Corte Interamericana de Derechos Humanos

La Corte Interamericana de Derechos Humanos (CIDH) declaró culpable a Brasil en julio de 2009, y ordenó compensación a favor de los trabajadores de las cooperativas agrícolas asociadas con el *Movimento Sem-Terra*, a causa de operaciones de interceptación telefónica indebida llevadas a cabo por el Estado de Paraná en 1999.[29] Dichas operaciones de interceptación, que duraron 49 días, se dieron mediante orden judicial sin que haya fundamentos jurídicos adecuados, bajo la solicitud de una autoridad inapropiada (Policía Militar), fuera del ámbito de una investigación en curso, y sin notificar a la Fiscalía General, todo en violación de la Ley de Interceptación Telefónica. Adicionalmente, los fragmentos de interceptación protegidos por procedimientos *a puerta cerrada* se revelaron y posteriormente se divulgaron en una conferencia de prensa convocada por el Secretario de Seguridad Pública del Estado de Paraná días después de las grabaciones, lo cual también se encuentra en violación de la Ley de Interceptación Telefónica.

Para peor, las autoridades involucradas en la interceptación ilícita no se consideraron responsables por ninguna Corte brasileña. Según la CIDH, Brasil violó el derecho a la vida privada de las víctimas, su honor, y su libertad de asociación, además de las protecciones y garantías brindadas por la Convención Interamericana de Derechos Humanos. Las *Resoluções* del CNJ y el CNMP pueden verse en contexto en este caso.

La CIDH también reconoció de manera expresa que el derecho a la privacidad abarca no solo la protección del contenido de las comunicaciones sino también de los metadatos: "[El derecho a la privacidad] puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación".[30]

¿Hay software espía de la policía en teléfonos móviles hacekados?

En abril de 2015, un artículo publicado por el diario *Folha de São Paulo* reveló que la Policía Federal está tratando de incrementar el acceso a la información almacenada en los teléfonos móviles sujeto a interceptaciones mandadas por orden judicial.[31] Esto es así porque, actualmente, la tecnología implementada en las operaciones de interceptación solamente puede acceder a los mensajes de texto SMS y llamadas, pero no a los mensajes enviados a través de aplicaciones de mensajería basadas en Internet, como WhatsApp, cuyo uso ha

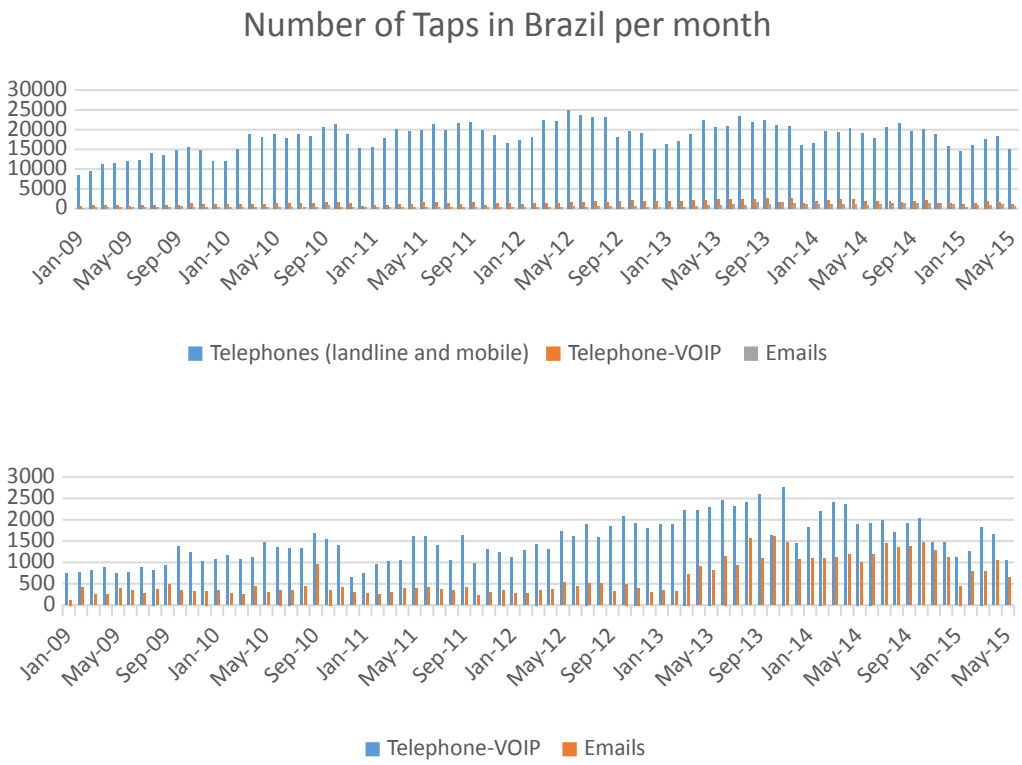
crecido. Este artículo indica que la Policía Federal "quiere que las compañías telefónicas compren programas espías", a lo cual estas compañías se oponen, debido a los altos costos de adquisición de los programas y del uso de los paquetes de datos de los subscriptores para transferir información copiada de aquellos que están siendo investigados. Adicionalmente, el artículo menciona que durante la operación *Lava Jato*, la cual reveló el escándalo de corrupción en la empresa estatal de petróleos Petrobras, la Policía Federal solamente pudo acceder a los mensajes de Alberto Youssef, traficante del mercado negro, "porque convenció a BlackBerry de que le concediera acceso a las conversaciones vía BBM, un servicio de mensajería instantánea de los dispositivos BlackBerry".

El artículo recalca, por un lado, la necesidad de regulación en este tipo de datos a los cuales se concede el acceso mediante la interceptación, con el objeto de cumplir con los principios de legalidad y proporcionalidad aplicables a las limitaciones de los derechos fundamentales y, por lo tanto, establecer los límites que habiliten tener control sobre el poder del Estado.

El uso de malware, incluso dentro del ámbito de una orden judicial para las operaciones de interceptación en investigaciones en curso, como aquellas que menciona el artículo de noticias, genera una preocupación que excede a la confidencialidad de las comunicaciones y afecta la integridad de las comunicaciones y sistemas.[32] (Al respecto, véase *¿Cooperación con Hacking Team?* presentado más abajo). Por otro lado, el artículo también muestra cómo la deficiencia normativa da lugar a "acuerdos no reglamentarios" para la obtención de datos protegidos por los derechos a la confidencialidad de las comunicaciones y a la privacidad.

Sistema Nacional para el Control de Interceptaciones

Gracias a las disposiciones de la *Resolução* nº 59/08 emitida por el CNJ, 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. Dichos datos no están disponibles para el público en general y fueron obtenidos por InternetLab mediante la Ley de Acceso a la Información.[33]



Las tablas muestran que la cantidad promedio de líneas telefónicas bajo vigilancia en Brasil mensualmente excede las ocho mil. También se puede ver que el número de direcciones de correo electrónico y teléfonos VoIP ha crecido en los últimos meses. Para explicar qué representan estas y otras cifras recopiladas por el Sistema Nacional de Control de Interceptaciones con respecto a la aplicación de la Ley de Interceptación Telefónica por parte de las cortes brasileñas, sería necesario tener acceso al número total de solicitudes de interceptación emitidas o, en todo caso, al número de solicitudes de interceptación rechazadas por los jueces.

La comparación de Brasil con relación a otros países no ayuda con esta evaluación, pues hay una falta de equivalencia en los criterios de preparación de estadísticas. Se sabe que en el año 2013, la cantidad de órdenes de escucha autorizadas en los Estados Unidos, un país con una población de 120 millones de personas más que en Brasil, fue de 3.576.[34] No existe información sobre la cantidad de órdenes judiciales para interceptación autorizadas en Brasil, pero sí se sabe que se presentaron 13.309 procedimientos de interceptación penal nuevos en el 2013.[35] 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.[36] En Brasil, se conoce que se enviaron 50.265 notificaciones de interceptación a las compañías de telecomunicaciones durante el mismo periodo de tiempo.[37]

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, la protección teórica que 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 aplica 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.

2.6. Vigilancia carente de transparencia con propósitos de inteligencia y seguridad nacional

Alcance del Sisbin (Sistema brasileño de inteligencia)

La Ley nº 9.883/99 creó el Sistema brasileño de Inteligencia (Sisbin) para integrar la planificación y realización de tareas de inteligencia en Brasil, con el objeto de brindar al Presidente de Brasil subsidios en materia de interés nacional, para obtener, revisar y diseminar conocimiento relevante para las acciones del gobierno y los procesos de toma de decisiones, así como también asegurar la seguridad social y estatal (artículo 1).

El Sisbin está conformado por todos los organismos de la Administración Pública Federal responsables de producir conocimiento relevante para las actividades de inteligencia (artículo 2) especificados en el artículo 4 del Decreto nº 4.376/02, incluyendo a la Oficina del Jefe de Gabinete, el Gabinete de Seguridad Institucional de la Presidencia de la República, los Ministerios de Justicia, Defensa, Relaciones Exteriores, Salud, Finanzas, Ciencia y Tecnología, entre otros, y organismos relacionados, como el Departamento de la Policía Federal, el Departamento Nacional Penitenciario, el Departamento de Asistencia Legal Internacional, la Secretaría de Ingresos Federales de Brasil y el Banco Central. El principal órgano es la Agencia de Inteligencia de Brasil (ABIN), competente para planificar, realizar, monitorear y controlar las actividades de vigilancia.

La ABIN puede tener acceso a los datos obtenidos por otras autoridades mediante la cooperación en el SISBIN. El artículo 6, apartado V, del Decreto 4.376/02 que regula la operación del Sisbin, determina que los organismos de este sistema deben intercambiar y brindar la información solicitada para dar conocimiento de las actividades de inteligencia. El artículo 6-A del mismo Decreto, agregado en 2008, establece que la ABIN debe tener representantes en los organismos del Sisbin en el Departamento de Integración del Sisbin, los cuales "tendrán el derecho de acceder, a través de medios electrónicos, a las bases de datos de sus organismos de origen, sujeto a las normas y límites de cada institución y a las leyes de seguridad, secreto profesional y protección de cuestiones confidenciales" (inciso 4). Sobre esta base, es posible que la ABIN tenga acceso a información y datos originariamente

protegidos por el derecho a la confidencialidad de las comunicaciones, expandiéndose así las posibilidades de vigilancia por parte del Estado brasileño.

A pesar de que la ABIN no es competente para participar directamente en las actividades de interceptación, por ejemplo, porque ni la Constitución ni la Ley de Interceptación le concedieron propósitos de inteligencia,[38]no debe descartarse la posibilidad del acceso a datos por tareas de cooperación. El diario *Folha de São Paulo* divulgó un caso en 2008 que reveló este tipo de acceso indirecto de la ABIN a las comunicaciones interceptadas disponibles en un Sistema de la Policía Federal (*Guardião*).[39] En el caso de que la Secretaría de Ingresos Federales de Brasil posea documentos de facturación de compañías telefónicas, la ABIN tendría permitido el acceso a los registros telefónicos de los usuarios.

La Ley nº 9.883/99 obliga al Sisbin, como regla general, y a la ABIN, en particular, a que cumplan con los derechos y garantías Constitucionales al llevar a cabo sus actividades (artículo 1, inciso 1 y artículo 3, párrafo único), sujetas al control y monitoreo de la Comisión Conjunta para el Control de las Actividades de Inteligencia (*Comissão Mista de Controle das Atividades de Inteligência*), una comisión permanente del Congreso brasileño (artículo 6). La falta de transparencia sobre cómo tiene lugar la cooperación en el Sisbin evita realizar una evaluación más precisa de la ABIN en materia de vigilancia con propósitos de inteligencia y rodea a estas actividades de sombras e incertidumbres.

¿COLABORACIÓN CON HACKING TEAM?
un aporte de Artigo 19 y la Oficina Antivigilância

El 5 de julio de 2015, la compañía italiana *Hacking Team*—conocida por desarrollar y vender software espía y herramientas de vigilancia a los gobiernos y por ayudar a las instituciones militares y de aplicación de la ley a espiar computadoras, tabletas, y teléfonos celulares de ciudadanos de todo el mundo—fue *hackeada*. Como consecuencia, 400 Gigabytes de documentos internos, inclusive correos electrónicos privados, facturas, listas de clientes, y códigos fuente de productos comerciales se pusieron a disposición en todo Internet.

La documentación revelada contenía varias referencias a los organismos de Inteligencia brasileños, tanto civiles como militares, así como también a compañías de Brasil que aparentemente eran socios locales de Hacking Team. Entre los organismos que se mencionan en el archivo están: La Agencia Brasileña de Inteligencia (ABIN),[40] el Ejército del Centro de Inteligencia (CIE),[41] el Centro de Instrucción de Ciberguerra (CIGE),[42] el Departamento de la Policía Civil de Río de Janeiro (CINPOL[43] y DRCI[44]), el Departamento de la Policía Militar de Río de Janeiro [45], el Departamento de la Policía Civil de São Paulo[46], el Departamento de la Policía Civil de São Paulo[47], el Departamento de la Policía Civil del Distrito Federal,[48] el Departamento de la Policía Militar del Distrito Federal,[49] el Ministerio de Justicia,[50] y la Fiscalía General de la República.[51]

El archivo es extensivo y requiere una revisión cuidadosa, incluyendo la confirmación de la autenticidad de cada documento, y, por el momento, no se ha podido afirmar que dichas agencias hayan logrado adquirir "soluciones" desde la compañía italiana. La única excepción parece ser la Policía Federal, [52] ya que una inspección de los archivos, aunque haya sido superficial, reveló el intercambio de correos electrónicos entre agentes y empleados de Hacking Team,[53] reportes de entrenamientos en Brasília,[54] y diferentes documentos, incluso un certificado de entrega de producto,[55] lo que confirma la negociación y adquisición del sistema RCS (*Sistema de Control Remoto*) de Hacking Team para un proyecto piloto de tres meses.

Aun cuando estos documentos fueran auténticos, lo que no está claro es qué procedimientos administrativos se siguieron para completar la compra. En los correos electrónicos, solo existe la referencia a la Ley nº 13.097, el 19 de enero de 2015, la cual renuncia a procedimientos de licitación para las compras de "equipos sensibles solicitados para investigaciones policiales". También hay una referencia a una orden judicial[56] que habría sido emitida en la primera mitad de 2015, que concedía a un Departamento de la Policía Federal los fundamentos legales para utilizar las soluciones compradas por 15 días (a partir de la infectación) en 17 teléfonos seleccionados.

El sistema RCS, según Hacking Team, es un sistema discreto basado en software espía, diseñado para atacar, infectar y monitorear computadoras[57] (Windows, Mac OS, Linux) y teléfonos inteligentes (Android, BlackBerry, Windows Phone e iOS liberados). Esta herramienta permite rastrear y controlar los datos y las actividades de un dispositivo infectado: es posible ver los archivos guardados y cuáles fueron abiertos, borrados o imprimidos recientemente; activar el micrófono y la cámara y capturar imágenes o sonidos; acceder a los chats, correos electrónicos, SMS, y la ubicación; escuchar conversaciones vía Skype (VoIP) y llamadas de voz telefónicas; e incluso capturar cada pulsación de teclas. El RCS utiliza múltiples técnicas de infección que pueden ser físicas o remotas: a través de dispositivos de almacenamiento USB; redes Wi-Fi; adjuntos en correos electrónicos; y simples enlaces a sitios falsos.

En términos generales, los documentos filtrados plantearon aun más preguntas con respecto al creciente mercado de vigilancia en Brasil y señalaron la necesidad de que existan debates legales sobre el tipo de datos a los que se puede acceder mediante interceptación, teniendo en cuenta particularmente el avance de las nuevas tecnologías de vigilancia. Los 400 GB parecen reconfirmar la información publicada en abril de 2015 por el diario *Folha de São Paulo* sobre la intención de la Policía Federal de utilizar, sin orden judicial, una "aplicación especial" para recopilar datos de los teléfonos investigados.[58]

2.7. Vigilancia de comunicaciones públicas

Más abajo se presentan tres casos prácticos de monitoreo de las comunicaciones encontrados de manera pública en Internet. Aunque no plantea preguntas sobre confidencialidad de las comunicaciones y privacidad, este tipo de vigilancia por parte de diferentes entidades gubernamentales tiene el potencial de obstaculizar el ejercicio de las libertades, particularmente de la libertad de expresión, de reunión y de asociación.

Riesgo para la libertad de expresión: #HumanizaRedes

El Pacto Nacional en contra de las Violaciones de los Derechos Humanos en Internet (*Pacto Nacional de Enfrentamento às Violações de Direitos Humanos na Internet*) - #HumanizaRedes es un programa del Gobierno Federal de Brasil creado mediante la *Portaria Interministerial* nº 3, el 8 de abril de 2015. Su objetivo es "fomentar el uso seguro y responsable de las funciones y aplicaciones de Internet, recibir y resolver quejas relacionadas con crímenes y violaciones de los derechos humanos y promover un ambiente digital sin discriminación" (artículo 1). Además de promover la educación sobre los derechos humanos y el uso seguro de las redes a través de material disponible en la plataforma #HumanizaRedes y redes sociales asociadas, el programa también aspira a "confrontar las violaciones de los derechos" a través de un canal en línea para la recepción de quejas de violaciones de derechos humanos en línea y fuera de línea.

Este programa fue recibido con reservas. El proyecto de Decreto Ley nº 47/2015[59] que presentó la Cámara de Diputados, que al cierre de esta edición está en espera de la opinión de la Comisión de Derechos Humanos y Minorías, por ejemplo, propone eliminar la norma que creó #HumanizaRedes a causa de que, entre otras razones, no establece criterios que definan qué tipo de comentarios deben considerarse una violación de los derechos humanos[60] y, en este sentido, le da inapropiadamente la responsabilidad de hacerlo al Poder Ejecutivo.

Sin embargo, la mayor preocupación en términos de vigilancia es qué incluirá el uso de software, que será elaborado con el Laboratorio de Imagen y Cibercultura de la Universidad Federal Espírito Santo para recopilar datos de perfil disponibles de manera pública en redes sociales que estén basados en la cuestión predefinida por la Secretaría de Derechos Humanos y trazar un mapa de violación de los derechos humanos en línea.[61] No existen disposiciones legales expresas que regulen la operación del programa, solo hay aclaraciones obtenidas a través de la Ley de Acceso a la Información, por la ONG Artigo 19.[62] En estas aclaraciones, la Secretaría de Derechos Humanos afirma que la operación, metodología y alcance del software, así como la [definición de la] cuestión que intentará identificar, siguen en discusión en el equipo de trabajo pertinente.

Vale la pena mencionar que, en principio, #HumanizaRedes solo maneja información que por lo general se encuentra disponible al público en línea, es decir, información a la que cualquier usuario puede acceder (como el contenido de perfiles públicos o blogs). Por lo tanto, no es un caso típico de vigilancia estatal de las comunicaciones; como regla, dicha vigilancia se enfoca en comunicaciones privadas. A pesar de esto, ya sea a través de la plataforma de quejas que crea o el software de monitoreo que usa, el programa puede generar *efectos inhibitorios* ("chilling effects" en inglés) en la libertad de expresión, garantizada por el artículo 5, apartado IV, de la Constitución Federal, al punto tal de que puede afectar a la libertad de los ciudadanos de publicar contenido en sus perfiles públicos.

Redadas Virtuales: la Policía en Facebook
un aporte de Artigo 19 y la Oficina Antivigilância

En 2013 y 2014, los oficiales de policía utilizaron varios criterios diferentes para identificar a los individuos que serían el blanco de las investigaciones de las grandes protestas que se daban en ese momento.[63]

El informe de investigación de la policía que llevó a la encarcelación o acusación de más de 20 manifestantes en Río de Janeiro, por ejemplo, revela que gran parte de la investigación se realizó a través del monitoreo de redes sociales; se consideraba que una persona era de interés en base a, en muchos casos, fotografías, etiquetas, y los amigos de Facebook del individuo.[64]

Las denuncias y citaciones en el ámbito de la investigación se basaron en la obtención de información a través de lo que se conoce como "Redadas virtuales",[65] actividad en la que el departamento de policía examinaba y revisaba no solo los perfiles personales de las personas de interés, sino también de sus parientes, amigos, o contactos de Facebook, teniendo en cuenta comentarios, "me gusta", o etiquetas en publicaciones y fotografías relacionados con las protestas.

La impresión que esto nos deja es que la mayor parte de la información recopilada venía de perfiles públicos de usuarios que no limitaron el acceso a través de la configuración de privacidad, lo cual facilitó el acceso de los oficiales de policía a esta información. No obstante, teniendo en cuenta la información mencionada en la investigación, no es posible determinar si este fue el único método utilizado o si también se crearon perfiles falsos y se enviaron solicitudes de amistad a los individuos de interés para examinar información no pública, práctica a la que Facebook se opuso públicamente[66] y que es objeto de recurso en el sistema jurídico de Brasil.

Además de monitorear los datos disponibles en redes sociales, en la misma investigación, la policía trató de obtener órdenes judiciales para tener acceso a los registros de acceso de al menos 46 perfiles, un grupo, y tres páginas de Facebook; y pidió específicamente "[...] información de cuenta que contenga los registros de creación y acceso, con la fecha, hora y referencia temporal, la dirección IP, e-mails principales y secundarios, números telefónicos de confirmación, así como también la información contenida en bases de datos (tarjetas de crédito, si el perfil maneja alguna página, etc) [...]." La solicitud también incluía a las comunicaciones hechas a través de la mensajería privada de Facebook, incluyendo datos como "textos, imágenes, archivos de audio, ubicación, etc." (sic), registrados desde marzo de 2013 hasta "la fecha en la que se conceda la solicitud".

Las redes sociales son espacios importantes en los que los ciudadanos ejercen su libertad de expresión y asociación. Las consideraciones de los derechos fundamentales y de los requerimientos del Código Procesal Penal aplican incluso al monitoreo estatal de datos de perfil disponibles públicamente. Algunas cuestiones importantes sobre esta forma de investigación incluyen su idoneidad y precisión, y las bases sobre las cuales las autoridades eligen comenzar las investigaciones. Estas también pueden llevar a los funcionarios a solicitar el acceso a registros no públicos; dicha solicitud también debe cumplir con los principios de necesidad y proporcionalidad.

"Mosaico" de la Agencia Brasileña de Inteligencia (ABIN): menos transparencia, más opacidad

En junio de 2013, el diario *O Estado de São Paulo* divulgó que la ABIN, a través de "un sistema online de monitoreo de sujetos" definido por el Gabinete de Seguridad Institucional (*Gabinete de Segurança Institucional*), conocido como "*Mosaico,*" estaría monitoreando las redes sociales, entre ellas Facebook, Twitter, Instagram y WhatsApp para revisar los movimientos de los manifestantes entre protesta y protesta, que en ese momento tenían lugar en todo el país.[67] Según se informa, el sistema tenía como objetivo "predecir el curso y magnitud de las protestas, la infiltración de partidos políticos, e incluso determinar las fuentes de financiamiento de los eventos". No es ilegal que el Estado tome conocimiento de las comunicaciones públicas y, a simple vista, el monitoreo de la ABIN no es claramente indebido.

Sin embargo, es importante hacer mención de dos aspectos. Primero, el artículo del diario sostiene que los mensajes privados, como los que se mandan por WhatsApp, también fueron monitoreados, lo cual constituye una interceptación del flujo de las comunicaciones, actividad en la que la ABIN no posee autoridad legal. Segundo, el artículo enfatiza la necesidad de transparencia en la operación del programa "Mosaico" de la ABIN y también en su alcance y propósito, lo que es esencial para el control significativo de la vigilancia de las comunicaciones por la autoridad en Brasil. [68]

3.
Recomendaciones

Este reporte presentó las prácticas y leyes de vigilancia de las comunicaciones en Brasil. Se identificaron los aspectos positivos de las leyes, así como también sus aspectos más problemáticos, ya sea en el contenido escrito de la ley o en la práctica de esta.

Concluiremos con el desarrollo de recomendaciones, usando los 13 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones como referencia:[69]

3.1 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

Legalidad

Las limitaciones a los derechos humanos deben ser prescritas por ley de manera clara y precisa; las leyes que limitan el derecho a la privacidad deben ser objeto de revisión periódica debido al ritmo de los cambios tecnológicos.

Objetivo legítimo

La vigilancia de las comunicaciones solo se permitirá para alcanzar un objetivo estatal legítimo.

Necesidad

El Estado tiene la obligación de probar que las actividades de vigilancia de las comunicaciones son necesarias para alcanzar un objetivo legítimo.

Idoneidad

Un mecanismo de vigilancia de las comunicaciones debe ser apropiado para cumplir con el objetivo legítimo.

Proporcionalidad

La vigilancia de las comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática. La vigilancia de las comunicaciones proporcionada necesitará la autorización previa de una autoridad judicial competente.

Autoridad judicial competente

Las decisiones relacionadas con la vigilancia de las comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente.

Debido Proceso

El debido proceso exige que cualquier interferencia con los derechos humanos esté enumerada apropiadamente en la ley, sea practicada consistentemente y estén disponibles para el público general en audiencia pública.

Notificación del usuario

Los individuos deben ser notificados de la decisión de autorizar la vigilancia de sus comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión, excepto en circunstancias particularmente excepcionales.

Transparencia

El gobierno debe proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, y la naturaleza de las actividades de vigilancia de las comunicaciones. El gobierno no debería interferir con los proveedores de servicios en sus esfuerzos para publicar los detalles del alcance y la naturaleza de sus propias transacciones con el Estado relacionadas con la vigilancia.

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. Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado.

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

Garantías para la cooperación internacional

En ocasiones, los Estados pueden necesitar la asistencia de un proveedor de servicios extranjero para realizar tareas de vigilancia. Esto debe ser regulado por acuerdos claros y públicos que garanticen el estándar disponible con el mayor nivel de protección en cada caso.

Garantías contra el acceso ilegítimo

Deben existir sanciones penales y civiles para las partes responsables de realizar vigilancia electrónica ilegal y aquellos afectados por la vigilancia deben tener acceso a los mecanismos legales necesarios para poseer medios de reparación. También se debe proveer una protección firme para los informantes que exponen actividades de vigilancia que amenazan a los derechos humanos.

3.2 Recomendaciones específicas

1) Promover cambios en la cultura legal: instruir a los estudiantes sobre temas de privacidad, confidencialidad de las comunicaciones, y libertad de expresión (especialmente en relación con la tecnología) y familiarizar a los futuros profesionales legales con el derecho internacional de derechos humanos, incluyendo a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, junto con su análisis legal y guía de implementación.

Uno de los problemas básicos que identificó este estudio fue la implementación de interpretaciones restrictivas de los derechos fundamentales reconocidos en la Constitución brasileña, lo cual amenaza la efectividad de la protección garantizada por tales derechos en la práctica. Esto lleva a la reducción de las protecciones de los datos de los usuarios de servicios de telecomunicaciones (incluso cuando se necesita una orden judicial para acceder a ellos).

Además, las estadísticas de interceptación telefónica en Brasil y el creciente número de correos electrónicos monitoreados, a pesar de la dificultad de sacar conclusiones válidas sobre estas cifras sin más información adicional, sugieren que la aplicación concreta del derecho internacional de derechos humanos en el contexto de la vigilancia puede no estar reflejada completamente en la práctica.

El fomento de la instrucción, explicación y debate aumentaría la concientización de estos temas y facilitaría la toma de decisiones fundamentadas sobre la vigilancia estatal, lo que es esencial para el cumplimiento real de la normativa legal en cuestión. Esto se puede lograr incrementando estos temas en los planes de estudio de las escuelas de derecho y proporcionando cursos y conferencias para mantener actualizados a los profesionales jurídicos, inclusive a los miembros del Poder Judicial y de la Fiscalía General.

2) Revisar los términos de las resoluciones (*Resoluções*) de la ANATEL que abordan la vigilancia de las comunicaciones y solicitar una forma de supervisión más transparente.

Las *resoluções* de la ANATEL imponen obligaciones con respecto a la identificación de los usuarios, la retención de datos, y la infraestructura de vigilancia, las cuales limitan los derechos fundamentales. Estas disposiciones se deben revisar. La resolución de la ANATEL nº 426/05, que regula la telefonía fija, no cumple con el principio de transparencia y precisión con respecto a la definición de los datos que requiere que sean almacenados y a la identificación de las autoridades que pueden tener acceso a dichos datos, lo cual es un problema, en vista del principio de legalidad.

Adicionalmente, la retención de registros según propósitos de Normativa de Telecomunicaciones debe ser limitada a aquellos que sean estrictamente necesarios para alcanzar dichos propósitos con el objetivo de cumplir con los principios de objetivo legítimo y necesidad. Deben reconsiderarse las obligaciones de retención de datos por cinco años. En Europa, esos periodos son mucho más cortos o son inexistentes: incluso bajo la directiva sobre Retención de Datos que ya fue reemplazada, el lapso variaba de seis meses a dos años.[70]

En ese sentido, en 2014, el Tribunal de Justicia de la Unión Europea (TJUE) declaró nula la Retención de Datos europea.[71] Sobre la cuestión en particular de si la interferencia que causa la directiva se limita a lo estrictamente necesario, el tribunal afirmó que "la directiva exige la retención de todo el tráfico de datos concernientes a la telefonía fija, móvil, acceso a Internet, e-mails y telefonía de Internet" y que "implica una interferencia en los derechos fundamentales de casi la totalidad de la población europea".[72] Recientemente, en julio de 2015, la European Digital Rights (EDRI), una alianza de más de 32 organizaciones sobre la privacidad y las libertades civiles en Europa, le pidió a la Comisión Europea que investigue las leyes de retención de datos ilegal en la Unión Europea después de la decisión del tribunal.[73]

A nivel internacional, el Alto Comisionado para los Derechos Humanos de la ONU declaró expresamente que "la retención de datos obligatoria de terceros, característica recurrente de los regímenes de vigilancia en muchos Estados, donde los gobiernos exigen a las compañías telefónicas y a los proveedores de servicios de Internet almacenar los metadatos de las comunicaciones y localizaciones de sus clientes para posterior aplicación de la ley y acceso de las agencias de inteligencia no resulta necesaria ni proporcional".[74]

Con respecto a la posibilidad de conceder el acceso directo a los registros telefónicos mediante la integración de los sistemas de la ANATEL con los de los proveedores esto es, como mínimo, cuestionable en vista del principio de transparencia. Las circunstancias en las que este acceso se conceda deben estar delimitadas de manera clara.

3) Monitorear el progreso de ADI 5063/DF, que impugna la constitucionalidad de los artículos 15 (acceso a la información de cuenta por parte de las autoridades policiales y la Fiscalía General bajo solicitud) y 21 (penalización por negativa a proveer el acceso) de la Ley de Organizaciones Criminales, y preparar intervenciones *amici curiae*.

La Ley de Organizaciones Criminales viola varios de los principios internacionales: legalidad (ninguno de sus términos es claro), necesidad (ordena la retención de registros telefónicos por cinco años sin evidencia empírica que apoye esta necesidad), proporcionalidad (no limita expresamente las circunstancias en las cuales se accede a los registros; impone sanciones de encarcelamiento y multa en caso no conceder el acceso), autoridad judicial competente (permite interpretaciones amplias con respecto a las clases de datos que pueden solicitar sin orden judicial) y notificación del usuario (no hay disposiciones sobre este asunto).

La actuación que impugna su constitucionalidad se enfrentará, por lo menos, con preguntas relacionadas con la necesidad y proporcionalidad de la obligación de retener los registros telefónicos y las circunstancias que permiten el acceso a los datos por parte de las autoridades competentes sin una orden judicial. En vista de lo anterior, la resolución sobre la constitucionalidad de esta ley será un antecedente importante para la protección y confidencialidad de las comunicaciones en Brasil. Es vital intervenir en este proceso. Hasta ahora, solo la Asociación Nacional de Delegados de la Policía Federal (*Associação Nacional dos Delegados de Polícia Federa*l) presentaron un escrito *amicus curiae.*

4) Regular el acceso a los metadatos de telefonía a través de legislación específica que considere la naturaleza sensible del caso.

El acceso a registros telefónicos no puede estar sujeto al trato informal que se le otorga en la Ley de Organizaciones Criminales, la cual solo ha hecho que el acceso sea más propenso al abuso y ha distanciado esta normativa aun más de los principios internacionales aplicados a la vigilancia de las comunicaciones. Lo ideal sería que el acceso a los metadatos de telefonía en Brasil estuviera sujeto a una normativa propia: una ley que establezca de manera clara los requerimientos para acceder (requerimientos formales, que delimiten expresamente cuáles son las autoridades competentes para presentar una solicitud y que determinen la necesidad de que medie una orden judicial, junto con requerimientos sustanciales que limiten tales accesos a tipos específicos de investigaciones), normas para la notificación del usuario, y transparencia sobre la cantidad y la frecuencia de las solicitudes. Las solicitudes de datos de ubicación también deberían ser abordadas de manera diferente de las que solicitan datos sobre las llamadas telefónicas del usuario.

Si la vigilancia se impone a través de la creación de la obligación de retención de datos, como lo hace la Ley de Organizaciones Criminales, la legislación debería al menos ser clara acerca del tipo de datos que se retendrán, respetar los principios de necesidad y proporcionalidad en términos de duración de la retención, definir de manera clara las normas para su acceso y uso, e incorporar normas para la seguridad de los datos. Solo así esta ley estaría más cerca de cumplir con los estándares internacionales de derechos humanos.

Tal y como lo afirmó el Alto Comisionado para los Derechos Humanos de la ONU: "mientras que las preocupaciones sobre la seguridad y la actividad criminal pueden justificar programas de vigilancia excepcionales y ajustados a las medidas de uso, la vigilancia sin garantías suficientes para la protección del derecho a la privacidad puede afectar de manera negativa el ejercicio de los derechos humanos y de las libertades fundamentales".[75]

5) Monitorear la aplicación del Marco Civil da Internet, supervisar el proceso de redacción de su regulación, y revisar la constitucionalidad del artículo 15.

El *Marco Civil da Internet* establece derechos y garantías importantes para la protección de los usuarios de Internet contra la vigilancia injusta de las comunicaciones, en particular porque contempla requerimientos claros sobre las circunstancias y requerimientos de acceso a los registros de conexión a Internet, el acceso a las aplicaciones, y a las comunicaciones privadas almacenadas. Mientras que el *Marco Civil da Internet* cumple con los principios de legalidad y autoridad judicial competente, esta teoría todavía no se ha hecho tangible. Por lo tanto, es vital monitorear la aplicación del *Marco Civil da Internet*.

En ese sentido, el *Marco Civil da Internet* todavía tiene cuestiones pendientes importantes: contempla la retención de datos obligatoria, pero no determina un periodo máximo después del cual los datos deben ser borrados —tampoco establece normas y estándares de seguridad para dichos datos (lo que pone en tela de juicio la proporcionalidad de esta obligación); no contiene normas en lo que respecta a la notificación del usuario sobre el acceso por parte de terceros a datos privados (lo cual es una clara violación al principio de notificación del usuario); no identifica de manera precisa quién es el sujeto de la obligación de mantener los registros de acceso a aplicaciones de Internet (lo cual representa un problema para el principio de legalidad). Consecuentemente, la sociedad civil debe seguir de cerca e intentar influenciar el proceso de redacción de la normativa del *Marco Civil da Internet*, que regulará estos aspectos.

Además, se deben reconsiderar los términos del artículo 15 del *Marco Civil da Internet*, que contempla la obligación de retención de registros de acceso a aplicaciones de Internet. Los datos a los que se refiere esta obligación pueden revelar información extremadamente sensible; se trata del comportamiento en línea y puede revelar intereses, hábitos, y relaciones personales. La existencia de medios que restrinjan menos los derechos fundamentales y que

puedan ofrecer la misma utilidad durante las investigaciones—como la posibilidad de ordenar la retención de datos solo bajo la sospecha fundamentada de que existe alguna actividad criminal por parte de un usuario de Internet—plantea preguntas sobre la necesidad de la medida existente. La retención de datos de cada usuario de telefonía o Internet de Brasil puede declararse inconstitucional en principio.

Si se considera constitucional, se debe modificar la ley para que se especifique que el acceso a los datos retenidos debe estar disponible solo en casos específicos de investigaciones penales relacionadas a crímenes graves, se debe reducir el plazo de retención, y se deben restringir los sujetos de la retención para minimizar el daño a los derechos de privacidad y de confidencialidad de las comunicaciones.

6) Monitorear la aplicación de la Ley de Interceptación Telefónica a las técnicas de vigilancia y a las nuevas situaciones.

Este reporte mostró que la Ley de Interceptación Telefónica se aplica no solo a las escuchas telefónicas, sino también a las telecomunicaciones. Además, describió los intentos de aplicación de la ley a nuevos métodos de vigilancia, como la infección de malware en teléfonos móviles y computadoras, lo que se demostró en el artículo e informe de la aparente cooperación de las autoridades brasileñas con Hacking Team. Este intento de amoldar la legislación para que incluya formas de vigilancia extremadamente distintas viola el principio de legalidad, y debe ser revisado: este tipo de tecnología no solo viola la confidencialidad de las comunicaciones, limitada por la Ley de Interceptación, sino que también plantea nuevos problemas con respecto a la protección de la integridad y la confidencialidad de los sistemas y, como mínimo, merece tener su propia normativa.

En el momento y en la medida de que los partidos fuera del gobierno tomen conocimiento de los casos que implican métodos de vigilancia nuevos, la aplicación e interpretación de la Ley de Interceptación puede y debe estar influenciada por la participación en causas judiciales, como la presentación de escritos *amici curiae*.

7) Realizar estudios empíricos de las solicitudes de acceso a información de cuenta y de violación de la privacidad de los metadatos presentadas por las autoridades policiales y la Fiscalía General; elaborar estadísticas sobre las violaciones a la privacidad de los metadatos; expandir y divulgar la información que se reciba desde el Sistema Nacional para el Control de Interceptaciones (Sistema Nacional de Controle de Interceptações);

Los cambios legales recientes le conceden a las autoridades policiales y a la Fiscalía General las facultades para acceder, bajo mera solicitud, a la información de cuenta y metadatos de

usuarios de telefonía.[76] Esto sugiere que *(i)* las investigaciones penales en Brasil dependen sustancialmente de la violación de la confidencialidad de la información de cuenta y metadatos, como resultado de deficiencias infraestructurales para emplear otros métodos de forenses informáticos y falta de personal; y/o que *(ii)* la lentitud del sistema judicial brasileño ha hecho que las autoridades que intervienen en las investigaciones busquen burlar al Poder Judicial al presionar para que haya cambios en la ley que les faciliten y aceleren el acceso a la información privada sin implicar a las cortes.

En ambos casos, está en riesgo la protección efectiva de los derechos a la confidencialidad de las comunicaciones y la privacidad, y la libertad de expresión. Llevar a cabo estudios empíricos sobre las prácticas concernientes a las solicitudes de acceso a información de cuenta y metadatos, elaborar estadísticas de estas, y entrevistar a los agentes involucrados puede apuntar a las razones subyacentes de esta situación y generar soluciones ampliamente aceptadas.

Al mismo tiempo, es crucial que los datos del Sistema Nacional para el Control de las Interceptaciones de la Oficina del Inspector General del Consejo Nacional de Justicia *(i)* estén generalmente a disposición del público sin necesidad de acudir a la Ley de Acceso a la Información, como fue el caso para obtener las estadísticas que se presentaron en este reporte; y *(ii)* sean expandidos: el sistema actual no proporciona información sobre la cantidad total de solicitudes de interceptación que se concedieron, solo ofrece la cantidad de actuaciones presentadas, evitando así el completo entendimiento del panorama de vigilancia. La transparencia significativa también exige que los datos sobre las interceptaciones recopiladas por el sistema del Consejo Nacional de la Fiscalía General estén disponibles al público.[77] No se puede ejercer un control de interceptaciones efectivo sin revelar estas cifras.

8) Impulsar la transparencia en la inteligencia y en las medidas de seguridad nacionales, crear estándares para la transferencia de datos dentro del Sisbin, e incrementar la supervisión.

Se sabe poco sobre las operaciones de la ABIN y el Sisbin en Brasil. Además, casi no hay información sobre la supervisión que lleva a cabo la Comisión Conjunta del Congreso Nacional. Solo ha salido a la luz un único programa de la ABIN para monitorear las comunicaciones públicas, lo cual llamó la atención del público debido a los recientes eventos de gran magnitud que tomaron lugar en Brasil.[78] La recomendación más básica parece ser prestar más atención a estos organismos, y exigir la transparencia de sus actividades para que puedan ser evaluados y estar sujetos al escrutinio público.

Este reporte mencionó que la ABIN no realiza interceptaciones, conforme a la ley, la jurisprudencia y la política de la ABIN. Es difícil creer que Brasil cuente con una autoridad de seguridad nacional que no intercepte las comunicaciones: una autoridad de vigilancia

que no vigile. Parece que esta incapacidad es (o puede ser) burlada a causa de la existencia del Sisbin. En vista de esto, es fundamental asegurar el cumplimiento de los principios internacionales sobre la vigilancia, la transparencia de las actividades llevadas a cabo por la agencia, y particularmente cómo esta coopera con el Sisbin y otros organismos, incluyendo a la Policía Federal y a la Secretaría de Ingresos Federales de Brasil.

Se deben crear estándares para las eventualidades de dicha cooperación, ya que el propósito de la recopilación de los datos de las comunicaciones (ya sea por parte de la Policía Federal para investigar casos penales, o por la Secretaría de Ingresos Federales de Brasil para el control fiscal o cuestiones de auditoría) puede ser distorsionado y dichos datos pueden ser usados con propósitos de inteligencia.

1 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, https://necessaryandproportionate.org/text Análisis Jurídico Internacional de Apoyo y Antecedentes, https://necessaryandproportionate.org/legalanalysis, Guía de Implementación de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf Consultado el 10 de septiembre 2015.

2 A los efectos de este reporte, el término "violación de la confidencialidad" se usa en un sentido amplio y hace referencia a las consecuencias de cualquier acción de divulgación (posterior a solicitudes u órdenes judiciales o cualquier otro tipo de solicitud de entrega de datos) de cualquier especie de información relacionada con las comunicaciones (información sobre la cuenta del usuario, metadatos o contenido). En el caso especial con respecto a la interpretación del artículo 5, apartado XII de la Constitución, este se refiere específicamente a cualquier procedimiento de interceptación que viole la confidencialidad de las comunicaciones.

3 Con respecto a la protección del flujo de las comunicaciones, vale la pena mencionar el trabajo de FERRAZ JR., Tercio Sampaio, "Sigilo de Dados: o direito à privacidade and os limites da função fiscalizadora do Estado," en: Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, 1993, p. 439-459. En lo que respecta al alcance de la excepción, véanse ambos: SILVA, José Afonso da. Curso de Direito Constitucional Positivo. 32ª Ed. São Paulo: Malheiros, 2008, p. 438; y FERREIRA FILHO, Manoel Gonçalves. Curso de Direito Constitucional. 35ª Ed. São Paulo: Saraiva, 2009, p. 301 concur.

4 En el juicio de Recurso Extraordinário 418.416-8/SC, del 10 de mayo de 2006, el caso presentado por el Juez Sepúlveda Pertence indica que la protección descrita en el apartado XII del artículo 5 no hace referencia a la información trasmitida por correspondencia, mensajes telegráficos, datos y llamadas telefónicas en sí, si no que se refiere a las comunicaciones que están en curso, al flujo de las comunicaciones mientras están en proceso. De manera implícita, esta decisión excluye la aplicación de la excepción sobre el flujo de datos expuesta en el apartado XII del artículo 5.

5 En el habeas corpus 70814/SP (Caso presentado por el Juez Celso de Mello, juicio del 1 de marzo de 2004), por ejemplo, la Corte Suprema Federal aceptó que una administración penitenciaria pudiera interceptar las cartas de los reclusos por razones de seguridad pública, disciplina penitenciaria o preservación del orden judicial, con base en el único párrafo del artículo 41 de la Ley nº 7210/84, Derecho Penal Penitenciario, que limita el derecho de los reclusos de "hacer contacto con el mundo exterior a través de la correspondencia" (artículo 41, XV de la misma Ley). Con respecto a este asunto, consulte MORAIS, Alexandre. Direito Constitucional. 28ª Ed. São Paulo: Atlas, 2012, p. 59. En el desarrollo de este reporte, se presentarán más disputas sobre la validez de una interpretación limitada del apartado XII del artículo 5.

6 Véase, por ejemplo, Corte Suprema Federal, Mandado de Segurança 24.817/DF, Caso presentado por el Juez Celso de Mello, juicio del 3 de febrero de 2005, el cual relaciona violaciones de confidencialidad de los registros fiscales, bancarios y telefónicos con las restricciones de los derechos contemplados por el artículo 5, X. Visite http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605418. Consultado el 17 de junio de 2015.

7 A los efectos de este reporte, la información de la cuenta hace referencia a la información incluida en los registros del usuario de la compañía telefónica, operador del sistema autónomo, o el proveedor de la aplicación.

8 A los efectos de este reporte, el término "metadatos" hace referencia a todos los datos y registros que se generan de una comunicación específica que no incluye el contenido, tales como la fecha, hora y duración de la comunicación, el emisor, receptor, ubicación geográfica del dispositivo, si se conoce (como los identificadores o medidores mediante una estación de base de radiocomunicaciones), códigos de identificación del dispositivo (como el IMEI), e información análoga.

9 Véase "Información protegida", Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. 10 de julio de 2013. Disponible en: https://necessaryandproportionate.org/text Consultado el 10 de septiembre de 2015.

10 Véase Luis Fernando Sarcia, The Metadata Debate. A Latin American Perspective (El debate sobre metadatos. Una perspectiva latinoamericana), 15 de septiembre de 2015. Disponible en: https://www.eff.org/deeplinks/2014/09/metadata-debate-latin-american-perspective. Consultado el 10 de septiembre de 2015. *Véase también* ACLU Vs Clapper. Declaración del Profesor Edward W. Felten, 26 de agosto de 2015. Disponible en: https://www.documentcloud.org/documents/781486-declaration-felten.html. Consultado el 10 de septiembre de 2015. *Véase* Clifton Parker, alumnos de Stanford demuestran que registros telefónicos pueden brindar una enorme cantidad de información, 14 de marzo de 2015. Disponible en: http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html Consultado el 10 de septiembre de 2015.

11 Las modificaciones legislativas recientes han "esquivado" la necesidad de que las órdenes judiciales obtengan información de cuenta, como se expone más adelante (sección 2.4: Vigilancia con y sin chequeos y balances: telefonía vs. Internet), contrariamente a lo expresado por la Corte Suprema Federal. Consulte Corte Suprema Federal, Recurso Extraordinário 716795/RS, Caso presentado por el Honorable Juez Luiz Fux, juicio del 31 de octubre de 2012, sobre la necesidad de que la policía solicite una orden judicial para obtener la información de cuenta de usuarios de telefonía; la Corte resolvió que es obligación solicitar una orden judicial, por la protección dispuesta en el artículo 5, X. Disponible en: http://stf.jusbrasil.com.br/jurisprudencia/22599582/recurso-extraordinario-re-716795-rs-stf Consultado el 17 de junio de 2015.

12 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y el Secretario General. Párrafo 19, 30 de junio 2014. Disponible en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf Consultado el 10 de septiembre de 2015.

13 FOLHA DE SÃO PAULO, "Anatel terá acesso total a dado sigiloso de telefones," publicado el 19 de enero de 2011. Disponible en: http://www1.folha.uol.com.br/fsp/mercado/me1901201103.htm Consultado el 17 de junio de 2015.

14 FOLHA DE SÃO PAULO, "Agência diz que não há quebra de sigilo, publicado el 19 de enero de 2011. Disponible en: http://www1.folha.uol.com.br/fsp/mercado/me1901201104.htm Consultado el 17 de junio de 2015.

15 GAZETA DO POVO, "Quebra de sigilo continua a depender de mandado judicial, diz Anatel", publicado el 21 de enero de 2011. Disponible en: http://www.gazetadopovo.com.br/economia/quebra-de-sigilo-continua-a-depender-de-mandado-judicial-diz-anatel-da8drvp4kj7uyodcxir2ijw3y Consultado el 17 de junio de 2015.

16 Consulte VARON FERRAZ, Joana., Boletín de Noticias nº 11 de la Oficina Antivigilância, disponible en: https://antivigilancia.org/pt/2015/07/novas-revelacoes-do-wikileaks-sobre-vigilancia-no-brasil-dilma-disse-que-nao-tem/. Vea también http://www.itamaraty.gov.br/index.php?option=com_content&view=article&id=10389:atos-assinados-por-ocasiao-da-visita-da-presidenta-dilma-rousseff-aos-estados-unidos-washington-30-de-junho-de-2015&catid=42&Itemid=280&lang=pt-BR#neutrinos-port-8 Consultado el 31 de julio de 2015.

17 En su momento, la Corte Suprema Federal asumió esta postura. Véase CORTE SUPREMA FEDERAL, Recurso Extraordinário 716795/RS, Caso presentado por el Honorable juez Luiz Fux, juicio del 31 de octubre de 2012, en el que se discute el requerimiento de una orden judicial solicitada por jefes de la policía civil para obtener la información de cuenta de los usuarios de teléfonos, y en el que se concluye que la orden judicial sí es necesaria. Disponible en: http://stf.jusbrasil.com.br/jurisprudencia/22599582/recurso-extraordinario-re-716795-rs-stf Consultado el 17 de junio de 2015.

18 Consulte ARAS, Vladimir. A investigação criminal na nova lei de lavagem de dinheiro. Boletim 237 do IBCCRIM. Disponible en: http://www.ibccrim.org.br/boletim_artigo/4671-A-investigao-criminal-na-nova-lei-de-lavagem-de-dinheiro Consultado el 17 de junio de 2015.

19 Las mociones de la ACEL (Asociación Nacional de Operadoras de Celulares) y ejemplos de notificaciones recibidas por las operadoras basadas en esa (interpretación de la) ley se pueden encontrar en el boletín de noticias CONJUR, "Operadoras reclamam de pedidos de delegados para quebra de sigilo telefônico", del 29 de octubre de 2014, disponible en: http://www.conjur.com.br/2014-out-29/telefonicas-reclamam-quebras-sigilo-pedidas-delegados Sobre la acción legal que interpuso la ACEL, consulte las noticias en el sitio web STF, disponibles en: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=254181 . Consultado el 31 de julio de 2015.

20 Francisco Brito Cruz, Director de InternetLab, informa que "en Brasil, Núcleo de Informação and Coordenação do Ponto BR (NIC.br), el brazo operacional del Comitê Gestor da Internet [Comité de Gestión de Internet] está a cargo de crear normas sobre cómo los proveedores de conexión a Internet pueden inscribirse como "sistemas independientes", y así participar en la asignación de direcciones IP realizada por el NIC.br. Según el NIC.br, las entidades deben tener, por ejemplo, "una red de infraestructura mínima" y " tener 2 o más conexiones independientes al Internet, o alternativamente, una conexión a un operador y otra a un punto de intercambio de tráfico", además de contar con una serie de estándares técnicos y el personal adecuado. Fuentes: <http://registro.br/tecnologia/provedor-acesso.html?secao=numeracao> y <ftp://ftp.registro.br/pub/gter/gter28/07-Asbr.pdf>." Por consiguiente, no todos los proveedores de Internet cumplen con la definición del *Marco Civil da Internet* que crea la obligación de retener los registros de conexión.

21 Véase BRITO CRUZ, Francisco, et. al., "¿Qué está en juego en la normativa del *Marco Civil da Internet*?, p. 32. Disponible en: http://www.internetlab.org.br/wp-content/uploads/2015/08/Report-MCI-v2-eng.pdf Consultado el 13 de septiembre de 2015.

22 Consulte http://participacao.mj.gov.br/marcocivil/pauta/acesso-a-dados-cadastrais-por-autoridades-administrativas/, http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/ y https://antivigilancia.org/boletim_antivigilancia/consultas/visualizacao. Consultado el 17 de junio de 2015.

23 Este argumento fue presentado por Google en una serie de casos. Antes del Marco Civil, el Tribunal Superior de Justicia (STJ, por sus siglas en portugués) abordó, en Inquérito nº 784-DF (Caso presentado

por la Jueza Laurita Vaz, juicio del 17 de marzo de 2013) esta cuestión y ordenó el acceso a los datos. Más recientemente, un juez federal falló a favor de Yahoo en una acción colectiva presentada por la Fiscalía General, que exigía a la compañía entregar los datos retenidos en su empresa matriz Yahoo INC. De acuerdo con la resolución judicial, Yahoo Brasil no posee el control sobre los datos que se almacenan en el exterior (en la empresa matriz), lo cual obliga a Yahoo Brasil a entregar los datos que solamente este tiene en su posesión (es decir, de los usuarios cuyas cuentas están registradas en yahoo.com.br y no en yahoo.com). Véase *26ª Vara Federal da Seção Judiciária de São Paulo, Ação Civil Pública nº 0012450-95.2014.4.03.6100 – Ministério Público Federal v. Yahoo! Do Brasil Internet LTDA*. Disponible en: http://www.internetlab.org.br/wp-content/uploads/2015/07/Y.SENTENÇA.ACP_.MPSP_.pdf Consultado el 13 de septiembre de 2015.

24 En febrero de 2015, el Juez Luiz Moura Correia, quien preside la Central de Inquéritos da Comarca de Teresina, ordenó el bloqueo de la aplicación de WhatsApp en Brasil debido a que la compañía al parecer no estaba cooperando con las investigaciones penales o cumpliendo con las órdenes de violación de confidencialidad. Consulte O ESTADO DE SÃO PAULO, "Juiz exige a suspensão do Whatsapp in Brazil," publicado el 25 de febrero de 2015, disponible en: http://blogs.estadao.com.br/link/juiz-exige-a-suspensao-do-whatsapp-no-brasil/ Consultado el 31 de julio de 2015. Esta resolución fue anulada por la Corte de Justicia del Estado de Piauí poco tiempo después. Vea el caso de Yahoo Inc, que InternetLab Blog abordó en el periódico Estado de São Paulo el 23 de julio de 2015, disponible en: http://blogs.estadao.com.br/deu-nos-autos/acesso-daqui-guardo-la-onde-estao-nossos-dados-na-internet/ Consultado el 31 de julio de 2015.

25 TRIBUNAL DE JUSTICIA DE RIO GRANDE DO SUL. Agravo de Instrumento nº 70018683508, Jueza de Corte de Apelaciones Maria Berenice Dias. Sentencia: 28 de julio de 2007. Disponible en: http://jus.com.br/jurisprudencia/16757/tjrs-authoriza-interceptacao-telefonica-para-localizar-devedor-de-alimentos Consultado el 17 de junio de 2015.

26 SALA DEL TRIBUNAL FEDERAL – TRIBUNAL DEL DSITRITO SÃO PAULO. Mandado de Segurança nº 0001972-91.2015.4.03.6100. Jueza Federal Djalma Moreira Gomes. Fecha de la Sentencia: 24 de abril de 2015. Disponible en: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/jfsp_00019729120154036100_24042015_KG45KXb.pdf. Consultado el 17 de junio de 2015.

27 CORTE SUPREMA FEDERAL. Ação Direta de Inconstitucionalidade ºnº 1488-9/DF, Juez Néri da Silveira. Sentencia del 7 de noviembre de 1999.

28 Véase, por ejemplo, CORTE SUPREMA FEDERAL, habeas corpus 84.301-SP, Juez Joaquim Barbosa, sentencia del 9 de noviembre de 2004 (disponible en: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79542; consultado el 3 de agosto de 2015) y Habeas Corpus 83.515-RS, Presentado por el Juez Nelson Jobim, sentencia del 16 de septiembre de 2005 (disponible en: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79377; consultado el 3 de agosto de 2015).

29 CORTE INTERAMERICANA DE DERECHOS HUMANOS. Caso Escher et al. vs. Brasil. Sentencia del 6 de julio de 2009. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf Consultado el 17 de junio de 2015.

30 CORTE INTERAMERICANA DE DERECHOS HUMANOS. Caso Escher et al. vs. Brasil: Excepciones Preliminares, Fondo, Reparaciones y Costas. Fallo del 6 de julio del 2009. Serie C Nº 200,

párrafo 114. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf Consultado el 17 de junio de 2015.

31 FOLHA DE SÃO PAULO, "PF quer instalar vírus em telefone grampeado para copiar informações," publicado el 27 de abril de 2015. Disponible en: http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml Consultado el 17 de junio de 2015.

32 Al respecto, véase MENDES, Laura Schertel, "Uso de softwares espiões pela polícia: prática legal?," en: Jota, publicado el 4 de junio de 2015, disponible en: http://jota.info/uso-de-softwares-espioes-pela-policia-pratica-legal, Consultado el 3 de agosto de 2015. Mendes enfatiza que la infección de dispositivos electrónicos a causa de troyanos es capaz de recopilar todos los fragmentos de información almacenados en el dispositivo. Esto va más allá de la interceptación del flujo de las comunicaciones regulada por la Ley de Interceptación Telefónica. También resalta que, en Alemania, una revisión de constitucionalidad de este tipo de procedimientos llevó a la Corte Constitucional Federal de Alemania a fallar para la existencia de un derecho fundamental para la fiabilidad y la integridad de los sistemas de tecnología de la información. *Véase también* Principio 11 - Integridad de las Comunicaciones y Sistemas, Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponible en: https://en.necessaryandproportionate.org/text#principle_11. Consultado el 10 de septiembre de 2015.

33 Ombudsman Registro/CNJ: 147763. Solicitud presentada por InternetLab al CNJ y respuesta respectiva, inclusive todos los datos sobre el sistema, disponible en: http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptance-para-o-site.pdf, consultado el 3 de agosto de 2015.

34 Consulte las estadísticas disponibles en: http://www.uscourts.gov/statistics-reports/wiretap-report-2013. Consultado el 3 de agosto de 2015. No obstante, cada orden de escucha puede incluir a más de una persona, por lo que pueden estar implicadas más de una línea telefónica.

35 Vea los datos del Sistema Nacional de Interceptação disponibles en: http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptance-para-o-site.pdf. Esta cifra se refiere a la cantidad de procesos penales presentados en 2013 llamados "iniciales", como lo muestra el cuadro: es decir, no se refiere al número total de procesos presentados en el mes, que puede incluir datos de meses anteriores. La tabla hace referencia a la información mensual en 2013 [sic] con respecto al ítem "Total 3", concerniente a la interceptación telefónica agregada a aquella del ítem "Total 9" concerniente a la interceptación telemática.

36 Vea las estadísticas disponibles en: https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2013.pdf?__blob=publicationFile&v=3 Consultado el 3 de agosto de 2015.

37 Vea los datos del Sistema Nacional de Interceptação disponibles en: http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptance-para-o-site.pdf. Esta cifra hace referencia a la cantidad de notificaciones emitidas en 2013, llamadas "iniciales", como lo muestra el cuadro: es decir, no hace referencia a las notificaciones emitidas durante ese mes, que puede incluir datos de meses anteriores. La tabla hace referencia a la información mensual en 2013 [sic] con respecto al ítem "Total 1", concerniente a la interceptación telefónica agregada a aquella del ítem "Total 7" concerniente a la interceptación telemática.

38 Esta opinión está manifestada en la jurisprudencia. Véase CORTE SUPERIOR DE JUSTICIA, habeas corpus 149250-SP, Juez Adilson Vieria Macabul, sentencia del 16 de mayo del 2012, en el que se revisaron

las operaciones de interceptación ilícita llevadas a cabo con los agentes de la ABIN en el ámbito de la Operação Satiagraha. La ABIN también mencionó esto de manera pública. Al responder la pregunta "A ABIN faz escuta telefônica?" (¿La ABIN intercepta conversaciones telefónicas?) en su sitio, la agencia indica: "La Ley nº 9.296, del 24 de julio de 1996, que regula el artículo 5, apartado XII de la Constitución Federal, determina los organismos competentes para realizar operaciones de interceptación telefónica, mediante orden judicial. La ABIN no está mencionada en esta disposición legal". disponible en: http://www.abin.gov.br/modules/mastop_publish/?tac=Perguntas_Frequentes (Consultado el 31 de julio de 2015). La agencia, sin embargo, fue acusada públicamente de haber interceptado el teléfono del Juez de la Corte Suprema Federal Gilmar Mendes, en un escándalo que se hizo público en 2008. Véase FOLHA DE SÃO PAULO, "Divulgação de grampo a presidente do STF derruba diretoria da Abin", publicado el 7 de noviembre del 2008, disponible en: http://www1.folha.uol.com.br/fsp/corrida/cr0709200802.htm Consultado del 31 de julio 2015.

39 FOLHA DE SÃO PAULO, "Acesso ao Guardião pela Abin gera polêmica", publicado el 12 de noviembre de 2008. Disponible en: http://www1.folha.uol.com.br/fsp/brasil/fc1211200805.htm Consultado el 13 de septiembre de 2015.

40 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/?q=%22ABIN%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Consultado el 13 de septiembre de 2015.

41 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/emailid/446716 Consultado el 13 de septiembre de 2015.

42 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/?q=%22CIGE%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Consultado el 13 de septiembre de 2015.

43 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/?q=%22CINPOL%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Consultado el 13 de septiembre de 2015.

44 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/?q=%22DRCI%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Consultado el 13 de septiembre de 2015.

45 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/emailid/7264 Consultado el 13 de septiembre de 2015.

46 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/emailid/7264 Consultado el 13 de septiembre de 2015.

47 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/?q=%22policiamilitar.sp.gov.br%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult Consultado el 13 de septiembre de 2015.

48 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/emailid/237181 Consultado el 13 de septiembre de 2015.

49 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/emailid/446822 Consultado el 13 de septiembre de 2015.

50 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/?q=%22mj.gov.br%22+!LISTA+!%22Progetto+Polizia+Federal%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=2#searchresult Consultado el 13 de septiembre de 2015.

51 Vea los resultados de búsqueda en: https://www.wikileaks.org/hackingteam/emails/emailid/446919 Consultado el 13 de septiembre de 2015.

52 Acceda a http://apublica.org/2015/07/hackeando-o-brasil/ Consultado el 13 de septiembre de 2015.

53 Acceda a http://htbrasil.pen.io/ Consultado el 13 de septiembre de 2015.

54 Véase https://www.wikileaks.org/hackingteam/emails/emailid/921981 Consultado el 13 de septiembre de 2015.

55 Vea el documento adjunto en: https://www.wikileaks.org/hackingteam/emails/emailid/921981 (documento adjunto) Consultado el 13 de septiembre de 2015.

56 Visite https://www.wikileaks.org/hackingteam/emails/emailid/921908 Consultado el 13 de septiembre de 2015.

57 Visite https://www.wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf Consultado el 13 de septiembre de 2015.

58 Vea FOLHA DE SÃO PAULO, "PF quer instalar vírus em telefone grampeado para copiar informações", publicado el 27 de abril de 2015. Disponible en: http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml Consultado el 13 de septiembre de 2015.

59 Con base en http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1214850. Consultado el 17 de junio de 2015.

60 El Equipo de Trabajo a cargo de #HumanizaRedes fue creado mediante la Portaria Interministerial nº 2, del 20 de noviembre del 2014. Su propósito es "recibir quejas sobre comentarios en línea posteados en redes sociales relacionadas con páginas web y sobre grupos que inciten o promuevan crímenes contra los derechos humanos, particularmente aquellos que fomenten la violencia en esencia discriminatoria" (cláusula principal del artículo 1). El único párrafo del artículo 1 define la incitación o la promoción de crímenes contra los derechos humanos como cualquier comentario que fomente cualquiera de los crímenes nombrados en la Ley nº 7.716, del 5 de enero de 1989 o en el artículo 40, párrafo 3, del Código Penal". El alcance de las actividades de #HumanizaRedes, por lo tanto, se atiene a esta definición.

61 BRAZILIAN FEDERAL GOVERNMENT, "Governo vai usar software contra crimes de ódio na internet," publicado el 12 de diciembre de 2014. Disponible en: http://www.brasil.gov.br/cidadania-e-justica/2014/12/governo-vai-usar-software-contra-crimes-de-odio-na-internet Consultado el 17 de junio de 2015.

62 Las solicitudes y respuestas a ARTIGO 19 se encuentran disponibles en: (i) http://www.artigo19.org/centro/esferas/detail/706; (ii) http://www.artigo19.org/centro/esferas/detail/701 y (iii) http://www.artigo19.org/centro/esferas/detail/702, consultados el 17 de junio de 2015.

63 Con respecto a las protestas, lea los detalles en: http://www.artigo19.org/protestos/

64 La Agencia Pública tenía acceso a los detalles de la investigación y recalcó estos aspectos en este artículo: http://apublica.org/2015/05/um-preso-politico-no-brasil-democratico/

65 "Virtual Raid" es básicamente un trabajo manual para revisar los perfiles de los individuos asociados con páginas web que apoyan manifestaciones e incitan la destrucción de propiedad, y que están en contra de la aplicación de la ley, etc. Práctica llevada a cabo por la policía ya mencionada con anterioridad (por ejemplo, http://oglobo.globo.com/sociedade/oab-rj-aciona-ministerio-publico-estadual-policia-civil-para-investigar-paginas-consideradas-racistas-13953005).

66 http://www.techtudo.com.br/noticias/noticia/2014/10/facebook-veta-uso-de-perfil-falso-pela-policia-apos-polemica-com-nomes.html

67 ESTADO DE SÃO PAULO, "Abin monta rede para monitorar internet". Disponible en: http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500 Consultado el 17 de junio de 2015.

68 Expertos debatieron estas preocupaciones en un artículo de la REVISTA GALILEO, "Mosaico, o 'Prism' brasileiro", sin fecha de publicación. Disponible en: http://revistagalileu.globo.com/Revista/Common/0,,EMI339490-17770,00-MOSAICO+O+PRISM+BRASILEIRO.html Consultado el 17 de junio de 2015.

69 https://pt.necessaryandproportionate.org/text

70 Véase Directiva 2006/24/EC sobre la retención de datos generados y procesados durante la provisión de servicios de telecomunicaciones, disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. Consultado el 3 de agosto de 2015.

71 Sentencia del Tribunal en Derecho Digital Irlanda vs Irlanda. Asuntos acumulados C-293/12 y C-594/12, 8 de abril del 2014. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=1245760. Consultado el 10 de septiembre de 2015.

72 EDRI. European Digital Rights pide a la Comisión europea investigar las leyes de retención de datos ilegal en la UE. 2 de julio de 2015. Disponible en: https://edri.org/edri-asks-european-commission-investigate-illegal-data-retention-laws. Consultado el 10 de septiembre de 2015.

73 Vea EDRI, Lista no exhaustiva de los Estados Miembros de la UE con legislación nacional contraria a la sentencia del TJUE de Derechos Digitales en Irlanda - Digital Rights Ireland Ltd (C-293/12). Disponible en: https://edri.org/files/DR_EDRi_letter_CJEU_Timmermans_20150702_annex.pdf

74 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y el Secretario General. Párrafo 26, 30 de junio de 2014. Disponible en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf Consultado el 10 de septiembre de 2015.

75 Navy Pillay, Jefa de derechos humanos de la ONU insta a la protección de los individuos que revelan violaciones a los derechos humanos, 12 de julio de 2013, disponible en: http://www.un.org/apps/news/story.asp?NewsID=45399. Consultado el 10 de septiembre de 2015.

76 Vea el Proyecto de Ley nº 8.040/14, que se origina en la Cámara de Diputados, e incluye el derecho al acceso directo a la información de cuenta de los usuarios de Internet por parte de la Policía Federal, disponible en: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=623798, y el Proyecto de Ley nº 494/08, que se origina en el Senado Federal, y que expande la obligación de retener registros de conexión a Internet y permite el acceso, bajo mera solicitud del departamento de policía o de la Fiscalía General, a la información de cuenta y "datos de conexión" en investigaciones de casos "que involucren a niños y adolescentes", disponible en: http://www.senado.gov.br/atividade/materia/getPDF.asp?t=55354&tp=1. Consultado el 31 de julio de 2015.

77 InternetLab también solicitó al Consejo Nacional del Defensor del Pueblo de la Fiscalía General el acceso a la información sobre las interceptaciones recopiladas por el sistema del CNMP. Sin embargo, se negó el acceso debido a los defectos de forma de la solicitud y porque la "información solicitada se encuentra protegida por la confidencialidad bajo los términos de la Ley". Vale la pena recordar que dichas cifras son una mera estadística y no dan lugar a la divulgación de casos específicos, lo que plantea una pregunta sobre la supuesta protección de la confidencialidad. Vea la solicitud y su respuesta en: http://ouvidoria.cnmp.gov.br//ticket.php?track=AD7GASR276&Refresh=40756 . Consultado el 31 de julio de 2015.

78 El sector de inteligencia adquirió mayor importancia con la Copa Mundial de Fútbol del 2014 y seguirá siendo importante durante los Juegos Olímpicos de Verano del 2016 en Río de Janeiro. Sobre su eficacia, vea FOLHA DE SÃO PAULO, "Ameaça de bomba na Copa mobilizou inteligência e deixou Dilma apreensiva," publicado el 14 de junio de 2015 . disponible en: http://www1.folha.uol.com.br/esporte/2015/06/1641861-ameaca-de-bomba-na-copa-mobilizou-inteligencia-e-deixou-dilma-apreensiva.shtml . Consultado el 31 de julio de 2015.