PARAGUAY

COMENTARIOS Y RECOMENDACIONES DE AMNISTIA INTERNACIONAL (AI) Y LA ORGANIZACIÓN TECNOLOGÍA, EDUCACIÓN, DESARROLLO, INVESTIGACIÓN Y COMUNICACIÓN (TEDIC) SOBRE EL PROYECTO DE LEY **"QUE ESTABLECE LA OBLIGACIÓN DE CONSERVAR LOS DATOS DE TRÁFICO".**

MAYO, 2015

I. INTRODUCCIÓN

Amnistía Internacional (AI) y la organización Tecnología, Educación, Desarrollo, Investigación y Comunicación (TEDIC), han preparado el presente documento público dirigido principalmente a los parlamentarios, y las parlamentarias del Paraguay, que debatirán en el mes de junio 2015 el proyecto de Ley "Que establece la obligación de conservar los datos de tráfico" (expediente S-146438).

En ese sentido, AI y TEDIC expresan formalmente su preocupación respecto al citado proyecto de Ley, que ya cuenta con media sanción dada por la Cámara de Senadores en el primer trámite constitucional y resolución de rechazo dada por la Cámara de Diputados en el segundo trámite constitucional (Resolución N° 1243 de 12 de marzo de 2015), encontrándose pendiente en la Cámara de origen para su tratamiento en el tercer trámite constitucional.

Amnistía Internacional (AI) y la organización Tecnología, Educación, Desarrollo, Investigación y Comunicación (TEDIC), reconocen que el Estado paraguayo tiene obligaciones en materia de investigación y sanción de los delitos penales, incluyendo aquellos cometidos a través de tecnologías de información y comunicación. Este compromiso deriva, entre otros, de instrumentos de derechos humanos tales como el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.

No obstante, cualquier medida en este sentido debe respetar y proteger los derechos humanos, incluyendo el derecho a la privacidad y sus garantías previstas en la Constitución de la República del Paraguay y en los tratados internacionales de derechos humanos ratificados, en particular la Convención Americana sobre Derechos Humanos (artículo 11) y el Pacto Internacional de Derechos Civiles y Políticos (artículo 17).

II. ANTECEDENTES

El citado proyecto de ley obligaría a las empresas proveedoras de servicios de internet a almacenar los datos de tráfico (metadatos), identificación y geolocalización de los usuarios por el término de un año, para la eventual utilización de tal información en el marco de investigaciones de carácter penal. Los datos que el proyecto de ley obligaría a conservar son aquellos generados en torno a cualquier conexión electrónica, que incluye la dirección de IP, origen y destino de la misma, hora y fecha de conexión y desconexión, nombre y domicilio del titular registrado al momento del establecimiento de la comunicación y los datos disponibles para identificar la zona geográfica y el equipo utilizado para la comunicación.

El carácter violatorio de este tipo de normas ya ha sido advertido por instancias del sistema internacional de protección de derechos humanos. El Relator Especial de las Naciones Unidas sobre la promoción y protección de la libertad de opinión y expresión, Frank la Rue, ha señalado que: *"Las leyes nacionales de conservación de datos son invasivas y costosas, y atentan contra los derechos a la intimidad y la libre expresión. Al obligar a los proveedores de*

servicios de comunicaciones a generar grandes bases de datos acerca de quién se comunica con quién telefónicamente o por Internet, la duración del intercambio y la ubicación de los usuarios, y a guardar esta información (a veces durante varios años), las leyes de conservación obligatoria de datos aumentan considerablemente el alcance de la vigilancia del Estado, y de este modo el alcance de las violaciones de los derechos humanos. Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental"[1].

Amnistía Internacional y Tedic hacen un llamado a las senadoras y los senadores a legislar sobre la materia garantizando el pleno respeto a los derechos humanos, en particular el derecho a la privacidad. Preocupa que el proyecto no incorpore las salvaguardias necesarias para que esta medida legislativa se adecue a las obligaciones internacionales que el Estado paraguayo ha adquirido en materia de derechos humanos.

III. ESTÁNDARES INTERNACIONALES DE DERECHOS HUMANOS SOBRE LA VIGILANCIA DE LAS COMUNICACIONES

El Relator Especial de las Naciones Unidas sobre la promoción y protección de la libertad de opinión y expresión ha señalado que *"La vigilancia de las comunicaciones debe considerarse un acto sumamente perturbador que podría suponer una injerencia en los derechos a la libertad de expresión y la intimidad, y que atenta contra los fundamentos de una sociedad democrática. La legislación debe estipular que la vigilancia de las comunicaciones por el Estado solo se realice en las situaciones más excepcionales y únicamente con la supervisión de una autoridad judicial independiente. La legislación debe incluir salvaguardias relativas a la naturaleza, el alcance y la duración de las posibles medidas, los motivos que se requieren para disponerlas, las autoridades competentes para autorizarlas y supervisarlas, y el tipo de reparaciones previstas en la legislación nacional"*[2].

Por su parte, la Corte Interamericana de Derechos Humanos ha definido que el derecho a la intimidad contenido en el artículo 11 de la Convención Americana tiene por objeto garantizar que las personas disfruten de un ámbito reservado de su vida inmune a la intervención, el conocimiento o la divulgación del Estado o de terceros[3]. En un caso contencioso reciente en el que se condenó al Brasil por el uso ilegal de escuchas telefónicas en un proceso penal, la Corte Interamericana señaló que el derecho a la privacidad protege tanto al contenido de la comunicación electrónica como a otros datos propios del proceso técnico de la comunicación, como los metadatos o datos de tráfico, entendidos éstos como *"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*

---

1 Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue.* A/HRC/23/40, 17 de abril de 2013, párr. 67.

2 Consejo de Derechos Humanos. *Ibídem.*, párr. 81.

3 Corte IDH. *Caso Fontevecchia y D'Amico vs. Argentina. Sentencia de 29 de noviembre de 2011 (Fondo, Reparaciones y Costas)*, párr. 48.

contenido de la llamada mediante la grabación de las conversaciones"[4].

La Corte Interamericana ha indicado que *"la fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. Este progreso, en especial cuando se trata de interceptaciones y grabaciones telefónicas, no significa que las personas deban quedar en una situación de vulnerabilidad frente al Estado o a los particulares. De allí que el Estado debe asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada"*[5].

En tal sentido, los Estados tienen el deber de adecuar sus normas y procedimientos de vigilancia de las comunicaciones con fines legítimos de investigación penal a estas garantías mínimas. Así, la Corte Interamericana señaló que *"en cuanto a la interceptación telefónica, teniendo en cuenta que puede representar una seria interferencia en la vida privada, dicha medida debe estar fundada en la ley, que debe ser precisa e indicar reglas claras y detalladas sobre la materia, tales como las circunstancias en que dicha medida puede ser adoptada; las personas autorizadas a solicitarla, a ordenarla y a llevarla a cabo; el procedimiento a seguir, entre otros elementos"*[6].

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) ha señalado a su vez que las intervenciones estatales en materia de seguridad en internet deben ser limitadas y proporcionadas, y procurar cumplir con fines legales precisos, que no comprometan las virtudes democráticas que caracterizan a la red[7]. Cualquier medida que pueda afectar la libertad de expresión en internet, entre ellas la vigilancia de las comunicaciones, debe satisfacer un triple test de legitimidad a saber: las restricciones deben estar establecidas en la ley en los términos más claros y precisos posible, perseguir una finalidad legítima reconocida por el derecho internacional y ser necesaria para alcanzar dicha finalidad. Cuando las restricciones obedecen a finalidades penales, a estos requisitos se deben agregar los propios del debido proceso y del principio de legalidad[8].

Esta Relatoría señaló que *"la ley debe autorizar el acceso a las comunicaciones y a datos personales sólo en las circunstancias más excepcionales definidas en la legislación. Cuando se invoquen causales más o menos abiertas como la seguridad nacional como razón para vigilar la correspondencia y los datos personales, la ley debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resulta legítimo. Su aplicación deberá autorizarse únicamente cuando exista un riesgo cierto respecto de los intereses protegidos, y cuando ese daño sea superior al interés general de la sociedad*

---

4 Corte I.D.H. *Caso Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009 (Excepciones Preliminares, Fondo, Reparaciones y Costas)*, párr. 114.

5 *Ibídem.*, párr. 115.

6 *Ibídem.*, párr. 131.

7 CIDH. Relatoría Especial para la Libertad de Expresión. *Libertad de Expresión e Internet*. OEA/Ser.L/V/II.CIDH/RELE/INF. 11/13. 31 de diciembre de 2013, párr. 120.

8 *Ibídem.*, párr. 122.

en mantener el derecho a la privacidad y a la libre expresión del pensamiento y circulación de información"[9].

IV. LOS PRINCIPIOS DE NECESIDAD Y PROPORCIONALIDAD PARA LAS MEDIDAS DE VIGILANCIA DE LAS COMUNICACIONES

Toda medida de vigilancia debe ser estrictamente necesaria y proporcional a un fin legítimo en virtud del derecho internacional de los derechos humanos, tal como la persecución del delito o la protección de la seguridad nacional. Asimismo, cualquier interferencia en las comunicaciones debe ser aquella menos intrusiva posible para alcanzar el fin legítimo. Las leyes y políticas que rigen cualquier interferencia con los derechos humanos, incluyendo el derecho a la privacidad, deben contener las salvaguardias necesarias para evitar cualquier abuso. Amnistía Internacional y Tedic consideran que las medidas de vigilancia masiva e indiscriminada no constituyen una medida necesaria y proporcional ante la interferencia que representan frente al derecho a la privacidad.

Las medidas de vigilancia o interceptación de las comunicaciones privadas de las personas son compatibles con los estándares constitucionales e internacionales de derechos humanos cuando reúnen simultáneamente los siguientes requisitos:

a) la reserva de ley, es decir que las restricciones a la vida privada deben estar expresamente establecidas y autorizadas por una ley, la que debe incluir la naturaleza, alcance y duración de las posibles medidas de vigilancia, las razones para su solicitud, las autoridades competentes para permitir, implementar y supervisar las medidas, así como el tipo de recursos para la protección de los datos de carácter personal;

b) las medidas de vigilancia deben justificarse en la estricta necesidad de una causa legítima en una sociedad democrática, como puede ser la persecución de crímenes que únicamente podrán ser esclarecidos, enjuiciados y sancionados mediante la prueba obtenida de la interceptación de la comunicación de la persona sobre quien pesa una sospecha razonable de su directa relación con la conducta que se prevé sancionar;

c) la supervisión judicial, las medidas de vigilancia deben ser ordenadas judicialmente por un ente independiente e imparcial, y estar sometidas a control judicial y a otros métodos de supervisión democráticos como las comisiones de investigación parlamentaria;

d) la especificidad, las medidas de vigilancia de comunicaciones deben ser dirigidas específicamente a la persona o grupo de personas que se sospecha están involucradas con la conducta investigada;

e) la proporcionalidad, las medidas de vigilancia deben ser aquellas que representen la

[9] *Ibídem.*, párr. 162.

menor interferencia posible para alcanzar el fin esperado, estar estrictamente limitada a los contenidos y al tiempo mínimo necesario para el logro de sus objetivos legítimos, debiendo preverse garantías para la estricta reserva sobre aquello que no haga relación con lo investigado;

f) la **protección judicial efectiva**, ya que las leyes deben prever garantías de tutela que protejan a las personas del abuso de la vigilancia, del mal uso de sus datos de carácter personal y, específicamente, de la obtención ilegal de información con fines de persecución penal, debiendo preverse que las pruebas obtenidas en violación a estas salvaguardias mínimas carezcan de valor en juicio.

La Constitución y los tratados internacionales suscriptos por el Paraguay garantizan la inviolabilidad de la vida privada y familiar, el domicilio y la correspondencia, obligando a los Estados a la protección de esta dimensión de la inmunidad personal frente a los propios órganos del Estado así como a los particulares. Específicamente, se recuerda que la conducta de las personas, en tanto no se afecte al orden público o a los derechos de terceros, está exenta del control de la autoridad pública (artículo 33 de la Constitución).

V. RECOMENDACIONES PARA LA ADECUACIÓN DE LA LEY AL MARCO CONSTITUCIONAL E INTERNACIONAL DE PROTECCIÓN A LOS DERECHOS HUMANOS

Amnistía Internacional y Tedic se encuentran preocupadas por la carencia de salvaguardias necesarias para asegurar el respeto y la protección de los derechos humanos en el proyecto de Ley de conformidad con las garantías básicas previstas en la Constitución y los tratados internacionales que el Estado paraguayo ha suscrito. En virtud de ello, se plantean a continuación una serie de recomendaciones para adecuar la propuesta de Ley al marco internacional de protección de los derechos humanos:

a) El proyecto obliga a establecer un dispositivo de retención masiva e indiscriminada de datos que afecta a todas las personas usuarias de internet. Esta información permite conocer circunstancias precisas de la vida privada de las personas cuyos datos son interceptados y almacenados, como por ejemplo sus lugares de residencia y tránsito habituales, relaciones sociales, hábitos de consumo y las personas con quienes se comunica. El proyecto no permite que el dispositivo propuesto pueda distinguir entre situaciones en las que esta vigilancia estaría justificada y aquellas en las que no, permitiendo de este modo una intrusión abusiva e ilegítima del control estatal en la vida privada de las personas.

   El proyecto de ley debería establecer una lista taxativa de circunstancias en las que una medida de vigilancia de comunicaciones podrá ser ordenada en el marco de una investigación penal, así como una enumeración lo suficientemente amplia de aquella información que está exenta del control de la autoridad judicial por no tratarse de datos que estén directamente vinculados al objeto de la investigación penal.

b) Los mecanismos de vigilancia de comunicaciones no plantean la autorización judicial previa. Por el contrario, esta es dispuesta con carácter obligatorio y con alcance masivo, bajo gestión de las empresas privadas prestadoras de servicio de acceso a internet y transmisión de datos. Al prescindir de la previa autorización y supervisión judicial, las medidas de vigilancia presentan un grave déficit en materia de protección de derechos humanos que comprometen la responsabilidad internacional del Estado y la validez de las investigaciones penales que se pretendan llevar adelante.

El proyecto de ley debería establecer como una garantía expresa que una medida de vigilancia de comunicaciones sólo podrá ser ordenada y supervisada judicialmente.

c) Las medidas de vigilancia tampoco son individualizadas ni específicas, dirigidas en particular a quienes se pretenda investigar sobre la base de una sospecha razonable de la comisión de un ilícito penal. En tal sentido, el proyecto plantea medidas de vigilancia indiscriminada que no son razonables ni necesarias en una sociedad democrática y que carecen de proporcionalidad.

El proyecto de ley debería establecer disposiciones para que las medidas de vigilancia, además de ser ordenadas judicialmente, sean dirigidas de manera específica y limitada a las personas que se encuentran bajo una investigación penal.

d) El artículo 6 del proyecto obliga a retener los datos por un periodo de 12 meses, en contravención con el derecho internacional de los derechos humanos. El proyecto tampoco permite disponer de medios técnicos adecuados que permitan distinguir aquella información judicialmente relevante de aquella que no lo es, para proceder a la destrucción de la información que no guarde relación con las cuestiones sometidas a investigación penal. En aquellos casos en que la retención de datos es justificada bajo el derecho internacional de los derechos humanos y se atiene a los principios de necesidad y proporcionalidad, deben existir mecanismos para la destrucción de la información almacenada tan pronto como sea posible, y como máximo, no más allá de lo que sea estrictamente necesario para alcanzar el objeto legitimo para el cual ha sido obtenida.

El proyecto de ley debería establecer plazos más breves y mecanismos más precisos bajo control estatal que garanticen que toda la información que no guarde vínculo con la investigación sea destruida.

e) El artículo 8° del proyecto de Ley coloca bajo responsabilidad de las empresas privadas prestadoras de servicio de acceso a internet y transmisión de datos la obligación de la conservación y protección de los datos interceptados de los usuarios, dejando a las personas afectadas sin un mecanismo efectivo de protección. El proyecto no contempla algún mecanismo de control judicial periódico o de control democrático independiente sobre la gestión de estas bases de datos, que quedan bajo gestión de las empresas privadas.

El proyecto debería contemplar mecanismos de control, custodia y preservación de los

datos que hayan sido colectados como consecuencia de las medidas de vigilancia legítima que hayan sido dispuestas. Estos mecanismos deben estar bajo gestión y responsabilidad estatal.

f) El artículo 9° y 10° del proyecto establecen sanciones a las empresas prestadoras de servicio de acceso a internet que incumplan con la obligación de retener los datos de tráfico. Para tal efecto, se faculta al ente administrativo correspondiente (la Comisión Nacional de Telecomunicaciones) a dictar reglamentos y aplicar sanciones administrativas de acuerdo a la Ley N° 642 De Telecomunicaciones. Sin embargo, no se disponen las garantías necesarias para la protección de los usuarios y las usuarias frente a los abusos o la violación de la confidencialidad de las comunicaciones, de conformidad con las obligaciones estatales en derechos humanos. Las personas que pudieran ser afectadas por el uso ilegal de sus datos personales o la violación de la privacidad de sus comunicaciones quedan expuestas a una situación de indefensión legal incompatibles con las obligaciones de la República del Paraguay en la materia.

   En este sentido, la Ley no contempla previsiones para la protección judicial efectiva de los datos de carácter personal y para la reparación del daño por el mal uso o la violación de la confidencialidad de las comunicaciones privadas. En particular, no se disponen garantías judiciales que permitan anular las pruebas que hayan sido obtenidas en violación de las salvaguardias mínimas que una ley de vigilancia de las comunicaciones debiera tener conforme a los estándares de derechos humanos (artículo 36 de la Constitución paraguaya).

   El proyecto de Ley debería establecer garantías para la tutela judicial efectiva de los datos de carácter personal, que permitan a las personas que hayan sido afectadas por una medida de vigilancia abusiva la debida restitución de sus derechos vulnerados y una reparación adecuada.

FIN//