MÉXICO D.F. A 27 DE NOVIEMBRE DE 2014

Instituto Federal de Telecomunicaciones
P R E S E N T E

CONSULTA PÚBLICA DEL ANTEPROYECTO DE LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA

Luis Fernando García Muñoz, a nombre propio y en atención a la consulta pública sobre el Anteproyecto de Lineamientos de Colaboración en Materia de Seguridad y Justicia publicada el 12 de noviembre de 2014 por este Instituto Federal de Telecomunicaciones (en adelante el "Instituto"), comparezco para someter a su consideración el análisis, comentarios y las propuestas de modificación que la Red en Defensa de los Derechos Digitales considera que resultan indispensables para que los lineamientos sean compatibles con las obligaciones de derechos humanos que posee este Instituto, en particular, respecto del derecho a la privacidad y la inviolabilidad de las comunicaciones privadas, las cuales se encuentran gravemente amenazadas por los artículos 189 y 190 de la Ley Federal de Telecomunicaciones (en adelante "LFTR") y que este Instituto tiene la oportunidad de mitigar a través de la adopción de diversas salvaguardas contra el abuso de estas medidas.

Indefinición de autoridades designadas

La Corte Interamericana de Derechos Humanos ha señalado que las medidas de restricción al derecho a la privacidad, en especial las medidas de vigilancia encubierta, deben ser precisas e

indicar reglas claras y detalladas sobre la materia[1], 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.[2]

Al respecto, el Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos han señalado en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión que:

> *"Los Estados deben garantizar que la intervención, recolección y uso de información personal (...) estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados. La ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación."*[3]

No obstante, la LFTR se refiere de manera genérica a "instancias de seguridad" sin que este concepto este definido en ningún ordenamiento jurídico. Lo anterior, provoca una gran inseguridad jurídica, lo cual constituye a su vez una violación alderecho a la privacidad. En este sentido, se sugiere que el Instituto establezca un registro público de autoridades designadas de manera que las usuarias de servicios de telecomunicaciones, así como los concesionarios y autorizados, tengan plena certeza respecto de la identidad de las autoridades con facultades para realizar alguna solicitud de geolocalización en tiempo real, de acceso al registro de comunicaciones y de intervención de comunicaciones privadas.

Ausencia de Control Judicial

El artículo Décimo Primero del Anteproyecto parece sugerir que la recolección, conservación y acceso a los datos a que se refiere la fracción II del artículo 190 de la LFTR no se encuentran

1 *Caso Escher y otros vs. Brasil*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 131.

2 *Caso Escher y otros vs. Brasil*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 131.

3 Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión del Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. 2013, párr. 8.

protegidas por el derecho a la inviolabilidad de las comunicaciones privadas reconocido en el artículo 16 constitucional.

En este sentido es preciso señalar que los datos cuya conservación se mandata en el artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión, han sido considerados tanto por la Suprema Corte de Justicia de la Nación (SCJN), como por la Corte Interamericana de Derechos Humanos (Corte IDH), como datos se encuentran protegidos por el derecho a la privacidad y la inviolabilidad de las comunicaciones privadas en igual sentido que el contenido de las comunicaciones. Por ejemplo, la SCJN ha establecido al resolver el Amparo en Revisión 1621/2010 y en la Contradicción de Tesis 194/2012 el siguiente criterio:

> *Época: Novena Época*
> *Registro: 161335*
> *Instancia: Primera Sala*
> *Tipo de Tesis: Aislada*
> *Fuente: Semanario Judicial de la Federación y su Gaceta*
> *Tomo XXXIV, Agosto de 2011*
> *Materia(s): Constitucional*
> *Tesis: 1a. CLV/2011*
> *Página: 221*
>
> *DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE IDENTIFICAN LA COMUNICACIÓN.*
>
> *El objeto de protección constitucional del derecho a la inviolabilidad de las comunicaciones privadas, previsto en el artículo 16, párrafos decimosegundo y decimotercero, de la Constitución Política de los Estados Unidos Mexicanos, no hace referencia únicamente al proceso de comunicación, sino también a aquellos datos que identifican la comunicación. A fin de garantizar la reserva que se predica de todo proceso comunicativo privado,* resulta indispensable que los datos externos de la comunicación también sean protegidos*. Esto se debe a que, si bien es cierto que los datos no se refieren al contenido de la comunicación, también lo es que en muchas ocasiones ofrecen información sobre las circunstancias en que se ha*

producido la comunicación, afectando así, de modo directo o indirecto, la privacidad de los comunicantes. Estos datos, que han sido denominados habitualmente como "datos de tráfico de las comunicaciones", deberán ser objeto de análisis por parte del intérprete, a fin de determinar si su intercepción y conocimiento antijurídico resultan contrarios al derecho fundamental en cada caso concreto. Así, de modo ejemplificativo, el registro de los números marcados por un usuario de la red telefónica, la identidad de los comunicantes, la duración de la llamada telefónica o la identificación de una dirección de protocolo de internet (IP), llevados a cabo sin las garantías necesarias para la restricción del derecho fundamental al secreto de las comunicaciones, puede provocar su vulneración.

Amparo directo en revisión 1621/2010. 15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

(énfasis añadido)

En igual sentido, la Corte IDH, en el caso Escher vs Brasil ha señalado que:

"El artículo 11 protege las conversaciones realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio o actividad profesional que desarrolla. De ese modo, el artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, 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."[4]

(énfasis añadido)

En este sentido, es claro que los datos cuya conservación se mandata en el precepto analizado se encuentran protegidos por la Constitución y los Tratados Internacionales de Derechos Humanos. Asimismo, resulta pertinente precisar que la interferencia con el derecho a la inviolabilidad de las comunicaciones ocurre desde el momento de la recolección y conservación de los datos que identifican la comunicación, independientemente de otras conductas que de manera autónoma también constituyen interferencias, como el tratamiento, revelación o transmisión de dichos datos. Lo anterior se desprende claramente del siguiente criterio emanado de la Primera Sala de la SCJN:

Época: Novena Época
Registro: 161334
Instancia: Primera Sala
Tipo de Tesis: Aislada
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo XXXIV, Agosto de 2011
Materia(s): Constitucional
Tesis: 1a. CLIII/2011
Página: 221

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SUS DIFERENCIAS CON EL DERECHO A LA INTIMIDAD.

A pesar de ser una manifestación más de aquellos derechos que preservan al individuo de un ámbito de actuación libre de injerencias de terceros -como sucede con el derecho a la intimidad, a la inviolabilidad del domicilio o la protección de datos personales-, el derecho a la inviolabilidad de las comunicaciones privadas

4 Corte IDH. *Escher y otros vs. Brasil.* Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 114.

posee una autonomía propia reconocida por la Constitución. En cuanto a su objeto, el derecho a la inviolabilidad de las comunicaciones se configura como una garantía formal, esto es, las comunicaciones resultan protegidas con independencia de su contenido. En este sentido, no se necesita en modo alguno analizar el contenido de la comunicación, o de sus circunstancias, para determinar su protección por el derecho fundamental. Este elemento distingue claramente al derecho a la inviolabilidad de las comunicaciones de otros derechos fundamentales, como es el de la intimidad. En este último caso, para considerar que se ha consumado su violación, resulta absolutamente necesario acudir al contenido de aquello de lo que se predica su pertenencia al ámbito íntimo o privado. En definitiva, lo que se encuentra prohibido por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en su párrafo decimosegundo, es la intercepción o el conocimiento antijurídico de una comunicación ajena. ***La violación de este derecho se consuma en el momento en que se escucha, se graba, se almacena, se lee o se registra -sin el consentimiento de los interlocutores o sin autorización judicial-, una comunicación ajena, con independencia de que, con posterioridad, se difunda el contenido de la conversación interceptada.***

Amparo directo en revisión 1621/2010. 15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

(énfasis añadido)

De esta forma, se concluye que la conservación de datos consagrada en el artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión constituye una interferencia con el derecho a la inviolabilidad de las comunicaciones, lo cual implica que las mismas tienen que estar justificadas comforme a los principios de idoneidad, necesidad y proporcionalidad, así como cumplir con los requisitos constitucionales específicos, en

concreto, la necesidad de autorización judicial federal para que pueda llevarse a cabo dicha interferencia.

En este sentido, no puede dejar de afirmarse, que la conservación indiscriminada de datos que prevé el artículo 190, fracción II de la LFTR es incompatible con las obligaciones de derechos humanos del Estado Mexicano. La incompatibilidad de las disposiciones de conservación obligatoria de datos con el derecho a la privacidad ha sido reconocido por el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas:

> *"Las leyes de retención de datos nacionales son invasivas y costosas, y amenazan los derechos a la privacidad y a la libertad de expresión. Al obligar a los proveedores de servicios de comunicación a crear grandes bases de datos con información acerca de quien se comunica on quien a través de un teléfono o de Internet, la duración de la comunicación, y la localización de las y los usuarios, y a conservar dicha información (en ocasiones por años), la leyes de retención obligatoria de datos incrementan el alcance de la vigilancia estatal de manera considerable, y por tanto el alcance de las violaciones a derechos humanos. Las bases de datos sobre datos de comunicaciones son, además, altamente vulnerables al robo, fraude y revelación accidental"*[5]

Asimismo, resulta determinante hacer referencia a la reciente decisión del Tribunal de Justicia de la Unión Europea en la que la Directiva de retención de datos europea, la cual inspiró la introducción de dicha figura en el orden jurídico mexicano en el año 2009, ha sido declarada inválida por vulnerar el derecho a la privacidad[6]. Lo anterior, incluso a pesar de que en dicha Directiva se establecen una cantidad de salvaguardas que no tienen paralelo a las disposiciones que se analizan.

En este sentido, la conservación indiscriminada y masiva de datos de comunicaciones, por un plazo amplio de veinticuatro meses, sin que la conservación de datos por mayor tiempo del

5 Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de Abril de 2013. A/HRC/23/40

6 TJUE. Sentencia en los asuntos acumulados C-293/12 y C-594/12. Digital Rights Ireland y Seitlinger y otros. 8 de abril de 2014. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=ES&cid=279012. Comunicado de Prensa. El Tribunal de Justicia declara inválida la Directiva sobre la conservación de datos. Disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf

necesario para la prestación de servicio de telecomunicaciones este justificada de manera específica y sin estar precedida de la autorización judicial federal que requiere el artículo 16 constitucion confirman que la disposición analizada es violatoria del derecho a la inviolabilidad de las comunicaciones privadas.

Ante ello, y en cumplimiento de las obligaciones de derechos humanos en cabeza de este Instituto derivadas del artículo 1° Constitucional, resulta indispensable que los lineamientos requieran una autorización judicial específica para la conservación de datos más allá de los estrictamente necesarios para la prestación del servicio de telecomunicaciones. Asimismo debe reconocerse la necesdad de autorización judicial federal para el acceso tanto a los datos conservados, como a los datos de localización geográfica en tiempo real de dispositivos de comunicación.

Medidas de transparencia insuficientes

Dada la naturaleza secreta y altamente invasiva de las medidas de vigilancia encubierta llevadas a cabo en el ejercicio de labores de seguridad y justicia, resulta indispensable el establecimiento de medidas para inhibir el abuso de dichas medidas. Una de esas medidas es la transparencia estadística.

En la resolución "El derecho a la privacidad en la era digital", adoptada por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013, se recomienda a los Estados establecer o mantener "mecanismos nacionales de supervisión independiente y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado"[7] Por su parte, el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas ha expresado que:

> "Los Estados deben ser completamente transparentes respecto del uso y alcance de los poderes y técnicas de vigilancia de las comunicaciones. Deben publicar, como mínimo, información agregada sobre el número de solicitudes aprobadas y rechazadas, una desagregación de las solicitudes por proveedor de servicios y por investigación y propósito.

7 ONU. Asamblea General. Resolución aprobada por la Asamblea General el 18 de diciembre de 2013. 68/167. El derecho a la privacidad en la era digital. A/RES/68/167. 21 de enero de 2014.

> Los Estados deben otorgar a los individuos suficiente información para permitirles comprender totalmente el alcance, naturaleza y aplicación de leyes que permiten la vigilancia de comunicaciones. Los Estados deben permitir a los proveedores de servicios la publicación de los procedimientos que aplican para manejar la vigilancia de comunicaciones estatal, adherirse a esos procedimientos, y publicar registros sobre la vigilancia de comunicaciones estatal. (...)"[8]

En este sentido, resulta indispensable que se introduzcan obligaciones de transparencia específica relacionadas con la vigilancia encubierta para llevar a cabo funciones de seguridad y justicia. En concreto es indispensable que el artículo Décimo Cuarto establezca de manera detallada la obligación de cada concesionario o autorizado a hacer público en un informe de transparencia semestral información detallada que permita evaluar la efectividad de las medidas y que permita detectar el uso irregular de ellas. De esta forma, la información que debe ser reportada debe ser mucho más detallada a solamente el número de solicitudes, como se refiere el artículo Décimo Cuarto del Anteproyecto. En concreto debe requerise de parte de los concesionarios y autorizados:

a) Número de solicitudes;
b) Tipo de medida solicitada;
c) Autoridad que lleva a cabo la solicitud;
d) Número de cuentas o usuarias afectadas por las solicitudes;
e) Tipo de información solicitada;
f) Fundamentación y motivación de la solicitud y la autorización;
g) Número de solicitudes cumplidas o rechazadas; y
h) En su caso, la duración autorizada para llevar a cabo la medida;

En el caso de las autoridades designadas debe establecerse la obligación de reportar la siguiente información:

I. En el caso de las instancias del poder ejecutivo federal, los poderes ejecutivos de los estados, el órgano ejecutivo del Distrito Federal y municipios que soliciten o lleven a cabo medidas de vigilancia encubierta:

8 Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de Abril de 2013. A/HRC/23/40

a) Número de solicitudes;
b) Tipo de medida solicitada;
c) Persona física o moral en posesión de los datos cuyo acceso se solicita;
d) Número de cuentas o usuarias relacionadas con las solicitudes;
e) Tipo de información solicitada;
f) Fundamentación y motivación para realizar la solicitud;
g) En los casos en que es necesaria la autorización judicial respectiva deberá indicarse si la solicitud fue autorizada o denegada; y
h) En su caso, la duración autorizada por la autoridad judicial o por la ley para llevar a cabo la medida.
i) El plazo para llevar a cabo la notificación a las personas afectadas por la medida determinada por la autoridad judicial o por la propia autoridad y si ésta se ha llevado a cabo.

II. En el caso de las instancias de procuración de justicia federal, de los estados y el Distrito Federal deberá indicarse, además de la información señalada en la fracción anterior, el delito cuya investigación motiva la solicitud y el estado de la averiguación previa dentro de la cual se ha llevado a cabo la solicitud.

Derecho de notificación diferida

La detección de un uso irregular de las medidas de vigilancia encubierta contempladas en los artículos 189 y 190 de la LFTR no es posible si las personas no tienen conocimiento, en ningún momento, de que su privacidad fue invadida. Lo anterior aunado a la ausencia de control judicial abre un campo amplio de arbitrariedad en el abuso de las medidas de vigilancia encubierta.

Una de las salvaguardas fundamentales para proteger el derecho a la privacidad, la protección de los datos personales, garantizar el debido proceso y el acceso a un recurso efectivo es el derecho de notificación a la o el usuario afectado. Es decir, la obligación de parte de la autoridad de notificar a una persona que su privacidad o datos personales fueron interferidos mediante una medida de vigilancia encubierta. Si bien, dicha notificación, evidentemente no puede llevarse a cabo de inmediato en tanto se podría frustrar el éxito de una investigación,

dicha notificación debe llevarse a cabo cuando no esté en riesgo una investigación, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento pueda generar un riesgo inminente de peligro a la vida o integridad personal de alguna persona.

Este derecho de notificación a las personas afectadas por medidas de vigilancia ha sido reconocido, por ejemplo, por el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas:

> *"Los individuos deben contar con el derecho a ser notificados que han sido sujetos de medidas de vigilancia de sus comunicaciones o que sus comunicaciones han sido accesadas por el Estado. Reconociendo que la notificación previa o concurrente puede poner en riesgo la efectividad de la vigilancia, los individuos deben ser notificados, en cualquier caso, una vez que la vigilancia ha sido completada y se cuenta con la posibilidad de buscar la reparación que proceda respeco del uso de medidas de vigilancia de las comunicaciones"*[9]
>
> *(énfasis añadido)*

Este derecho de notificación ha sido reconocido, además, por el Tribunal Europeo de Derechos Humanos, el cual determinó en el *Caso Ekimdziev vs. Bulgaria* que una vez que la vigilancia ha cesado y ha transcurrido el tiempo estrictamente necesario para que el propósito legítimo de la vigilancia no sea puesto en riesgo, la notificación al afectado debe llevarse a cabo sin dilación.[10] En este sentido, se propone el establecimiento de este derecho de notificación diferida a las usuarias afectadas por una medida de vigilancia encubierta.

Se propone la siguiente redacción:

Artículo XX. En el caso de los sujetos obligados que llevan a cabo medidas de vigilancia encubierta, deberán notificar a las personas afectadas por dichas medidas a través de medios apropiados.

La notificación se realizará dentro del plazo de seis meses contados a partir de que concluya

9 Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de Abril de 2013. A/HRC/23/40

10 TEDH. *Caso de la Asociación para la Integración Europea y los Derechos Humaos y Ekimdzhiev vs. Bulgaria.* Aplicación No. 62540/00. Sentencia de 28 de Junio de 2007.

el periodo autorizado por la autoridad judicial o por la ley por para llevar a cabo la medida de vigilancia encubierta.

La notificación a las personas afectadas podrá ser diferida cuando, a solicitud de la autoridad competente, la autoridad judicial que haya autorizado la solicitud o el Instituto, según corresponda, considere que sea necesaria para evitar poner en riesgo una investigación, exista riesgo de fuga o de destrucción de evidencia o exista un riesgo inminente de peligro para la vida o integridad personal de una persona.

La notificación deberá incluir el acceso a los materiales obtenidos a través de la medida de vigilancia e información suficiente que permita al afectado acudir a las instancias que en derecho corresponda.

En ningún caso el diferimiento de la notificación podrá exceder el plazo de 12 meses contado a partir de que concluya el periodo autorizado por la autoridad judicial o por la ley para llevar a cabo la medida de vigilancia encubierta.

Las personas físicas y morales que hayan colaborado para llevar a cabo la medida de vigilancia encubierta colaborarán para efectuar la notificación a que este artículo.