FUNDAMENTOS PARA LA INTERPOSICIÓN DE UNA ACCIÓN DE INCONSTITUCIONALIDAD EN CONTRA DEL ARTÍCULO 190 DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN

ANEXO TÉCNICO

El artículo 190 fracción I de la Ley Federal de Telecomunicaciones y Radiodifusión viola los artículos 1, 14, 16 y 17 de la Constitución; los artículos 1.1, 2, 8.1 y 11.2 de la Convención Americana sobre Derechos Humanos; y los artículos 2.3, 14 y 17 del Pacto Internacional de Derechos Civiles y Políticos.

El artículo 190 fracción I de la Ley Federal de Telecomunicaciones y Radiodifusión obliga a los concesionarios de telecomunicaciones y a los autorizados a colaborar en la localización geográfica, en tiempo real, de equipos de comunicación móvil en los siguientes términos:

> *"Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:*
>
> *I. Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes.*
>
> *Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable.*

El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna".

Respecto del precepto citado, se desarrollarán los argumentos que demuestran su inconstitucionalidad de la siguiente manera:

1. La localización geográfica, en tiempo real, de equipos de comunicación móvil establecida en el artículo 190 fracción I de la Ley Federal de Telecomunicaciones y Radiodifusión constituye una interferencia con el derecho a la privacidad.

2. El artículo 190 fracción I viola el derecho a la privacidad al no cumplir con el requisito de previsión en la ley, pues no establece de manera clara, precisa y detallada las autoridades que pueden llevar a cabo la medida, las circunstancias en las que puede llevarse a cabo la medida, el procedimiento para el tratamiento, transmisión y destrucción de los datos obtenidos ni se establecen límites temporales a la medida invasiva.

3. El artículo 190 fracción I no constituye una restricción necesaria o proporcional y por tanto viola el derecho a la privacidad, al debido proceso y a un recurso efectivo al no contemplar salvaguardas adecuadas para detectar e inhibir el abuso de la medida de vigilancia y al impedir el acceso de los ciudadanos a recursos para combatir y reparar violaciones a su derecho a la privacidad.

La localización geográfica, en tiempo real, de equipos de comunicación móvil, establecida en el artículo 190 fracción I, constituye una interferencia con el derecho a la privacidad

En primer lugar, resulta importante señalar que la localización geográfica en tiempo real de dispositivos de comunicación constituye una medida que **interfiere con el derecho a la privacidad de las personas de manera severa**, en tanto los datos de localización de un dispositivo móvil revelan datos altamente sensibles de una persona.

Al respecto, el Grupo de Trabajo sobre Protección de Datos establecido por el artículo 29 de la Directiva 95/46/CE del Parlamento Europeo ha señalado que:

"Los dispositivos móviles inteligentes están muy estrechamente vinculados a las personas porque la mayoría de ellas tienden a mantener su dispositivo móvil muy cerca de ellas, en el bolsillo, en el bolso o sobre la mesilla de noche.

Raramente ocurre que una persona preste su dispositivo a otra. La mayoría de las personas son conscientes de que su dispositivo móvil contiene una gran cantidad de información, desde mensajes electrónicos hasta fotografías privadas, o desde un historial de navegación por Internet hasta, por ejemplo, una lista de contactos.

Esto permite a los proveedores de servicios de geolocalización disponer de una panorámica detallada de los hábitos y pautas del propietario de estos dispositivos y establecer unos perfiles exhaustivos. A partir de un período de inactividad nocturna puede deducirse el lugar donde duerme la persona, y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa. El perfil puede incluir asimismo datos derivados de las pautas de movimientos de sus amigos, sobre la base de lo que se conoce como «gráfica social»[1]

Un modelo de comportamiento también podría incluir categorías especiales de datos, por ejemplo visitas a hospitales y lugares de culto, presencia en actos políticos o en otros lugares específicos que, verbigracia, revelen datos sobre la vida sexual. Estos perfiles pueden ser utilizados para tomar decisiones que afecten significativamente a su propietario."[2]

En este sentido, es claro que la localización geográfica, en tiempo real, de equipos de comunicación móvil, constituye una interferencia con el derecho a la privacidad de las personas. Si bien, el derecho a la privacidad no es un derecho absoluto y, por tanto, puede ser restringido, esto es solamente válido siempre que las injerencias no sean abusivas o arbitrarias; por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática.[3]

Es importante enfatizar que no basta con que las medidas persigan un fin legítimo, como lo puede ser la investigación y sanción de delitos, sino que debe cumplir con la totalidad de los requerimientos constitucionales y convencionales, lo cual no sucede en el caso del artículo 190 fracción I, como a

---

[1] «Gráfica social» es un término que indica la visibilidad de amigos en los sitios de redes sociales y la capacidad para deducir rasgos de comportamiento a partir de los datos de estos amigos.

[2] Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes del Grupo de Trabajo sobe Protección de Datos Establecido por el artículo 29 de la Directiva 95/46/CE del Parlamento Europeo.

[3] *Caso Tristán Donoso vs. Panamá*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 27 de enero de 2009. Serie C No. 193, párr. 56.

continuación se demuestra.

El artículo 190 fracción I no cumple con el requisito de previsión en la ley y por tanto viola el derecho a la privacidad reconocido en el artículo 16 constitucional, 11.2 de la Convencion Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos.

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[4], 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.[5]

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."*[6]

De igual manera, en el contexto de medidas de vigilancia encubierta, como la geolocalización, en tiempo real, de equipos de comunicación móvil, la ley debe ser lo suficientemente clara en sus términos para otorgar a los ciudadanos una indicación adecuada respecto de las condiciones y circunstancias en que las autoridades están facultadas para recurrir a dichas medidas.[7] Además, en

---

[4] *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.

[5] *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.

[6] 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.

[7] TEDH. *Caso de Uzun vs. Alemania.* Aplicación No. 35623/05. Sentencia de 2 de Septiembre de 2010, párr. 61; Caso de *Valenzuela Contreras vs. España.* Aplicación No. 58/1997/842/1048. Sentencia de 30 de Julio de 1998, párr. 46.

vista del riesgo de abuso que cualquier sistema de vigilancia secreta implica, las medidas deben basarse en una ley que sea particularmente precisa, en vista de que la tecnología disponible para realizar esas actividades continuamente se vuelve más sofisticada[8].

En este sentido, el artículo 190 fracción I de la Ley Federal de Telecomunicaciones y Radiodifusión incumple el requisito de previsión en la ley, en tanto no se encuentran detallados aspectos básicos sobre las condiciones y circunstancias en las que la localización geográfica, en tiempo, real de equipos de comunicación móvil puede llevarse a cabo.

En primer lugar, el artículo 190 fracción I contempla a las "instancias de seguridad" dentro de aquellas autoridades facultadas para obtener la localización geográfica, en tiempo real, de equipos de comunicación móvil, sin que dichas "instancias de seguridad" se encuentren definidas en la Ley Federal de Telecomunicaciones y Radiodifusión o en cualquier otro ordenamiento vigente, lo cual representa una clara violación del requisito de previsión en la ley de restricciones al derecho a la privacidad.

Asimismo, no se señalan de manera clara, precisa y detallada las circunstancias en las que las distintas autoridades pueden solicitar la localización geográfica, en tiempo real, de equipos de comunicación móvil. En el caso de las "instancias de seguridad", en tanto ni siquiera su identificación precisa se encuentra definida en las leyes. La indefinición de estas autoridades y de las circunstancias en las que las mismas pueden llevar a cabo la medida de vigilancia representan una grave omisión que obliga a que las referencias a dichas "instancias de seguridad" sean declaradas inconstitucionales y expulsadas del ordenamiento jurídico.

En el caso de las "instancias de procuración de justicia", ni el artículo 190 fracción I, ni el Código Nacional de Procedimientos Penales definen las circunstancias en las que el Ministerio Público puede válidamente solicitar la localización geográfica, en tiempo real, de equipos de comunicación móvil, lo cual incluso contraviene lo señalado por la Suprema Corte de Justicia de la Nación al resolver la Acción de Inconstitucionalidad 32/2012, pues en aquella decisión se resolvió que la localización geográfica, en tiempo real, de equipos de comunicación móvil, solamente podía considerarse constitucional si, *inter alia,* se limitaba su uso a situaciones excepcionales para la investigación de delitos particularmente graves definidos precisamente en la ley.

---

[8] TEDH. *Caso de Uzun vs. Alemania.* Aplicación No. 35623/05. Sentencia de 2 de Septiembre de 2010, párr. 61; *Weber y Sarabia vs. Alemania*. Aplicación No. 54934/00. Decisión de 29 de Junio de 2006. párr. 93.

Como ha sido señalado, ni el artículo 190 de a Ley Federal de Telecomunicaciones y Radiodifusión, ni el artículo 303 del Código Nacional de Procedimientos Penales, que entrarán en vigor de manera simultánea, definen esos supuestos y por ende se confirma la inconstitucionalidad de dichos preceptos legales.

Igualmente no se definen otras circunstancias como el procedimiento a seguir, el tratamiento de los datos de localización obtenidos, ni las salvaguardas necesarias para detectar e impedir el abuso de la medida de vigilancia. Dichas circunstancias deben estar establecidas de manera clara, precisa y detallada en una ley en sentido formal y material. La ausencia de tales precisiones conlleva la inconstitucionalidad del artículo 190 fracción I al violar el derecho a la privacidad de la ciudadanía reconocido en los artículos 6 y 16 de la Constitución, 11.2 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos.

El artículo 190 fracción I no establece salvaguardas adecuadas y efectivas contra el abuso de la localización geográfica, en tiempo real, de equipos de comunicación móvil y por tanto no constituye una interferencia necesaria y proporcional al derecho a la privacidad reconocido en el artículo 16 constitucional, 11.2 de la Convencion Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos y viola, a su vez, el principio de legalidad, las garantías del debido proceso y el derecho a un recurso efectivo reconocidos en los artículos 14 y 16 constitucionales, 8 y 25 de la Convención Americana sobre Derechos Humanos y 2.3 y 14 del Pacto Internacional de Derechos Civiles y Políticos.

La localización geográfica, en tiempo real, de equipos de comunicación móvil, al ser esa una medida de vigilancia encubierta que por su naturaleza se lleva a cabo en secreto, merece un tratamiento jurídico acorde a esa naturaleza, en concreto, el establecimiento de distintas salvaguardas adecuadas para inhibir los riesgos inherentes de abuso y arbitrariedad que conllevan este tipo de medidas, en tanto, la persona afectada, en este caso la o él usuario de los servicios de telecomunicaciones, no tiene posibilidad de conocer la interferencia, y por ende, no le resulta posible resistir algún abuso en dichas facultades.

Al respecto, el Tribunal Europeo de Derechos Humanos ha resaltado en su jurisprudencia reiterada que la existencia de salvaguardas adecuadas y efectivas resulta determinante para el

análisis respecto de la necesidad y proporcionalidad de legislaciones que facultan invasiones a la privacidad.[9] La relevancia de garantías efectivas en contra del abuso de medidas de vigilancia electrónica encubierta ha sido destacada recientemente por la Asamblea General de la Organización de las Naciones Unidas[10], el Relator Especial de la ONU para el Derecho a la Libertad de Expresión y Opinión[11], la Alta Comisionada para los Derechos Humanos de la ONU[12], la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos[13], así como por organizaciones de la sociedad civil y expertos que han recogido las mejores prácticas derivadas de la jurisprudencia y doctrina comparada y han elaborado los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones[14].

No obstante, el artículo 190 fracción I de la Ley Federal de Telecomunicaciones y Radiodifusión desatiende la obligación de establecer salvaguardas adecuadas y efectivas en contra del abuso de la localización geográfica, en tiempo real, de equipos de comunicación móvil.

En primer lugar, no se establece en dicho precepto, ni en el Código Nacional de Procedimientos Penales u otra legislación aplicable, la necesidad de obtener una autorización judicial para poder acceder a los datos de localización geográfica, en tiempo real, de equipos de comunicación móvil. Lo anterior permite que se lleve a cabo esta facultad y se mantenga en secrecía de manera indefinida, impidiendo que el afectado o un juez puedan evaluar la idoneidad, necesidad y proporcionalidad de la medida, detectar el ejercicio abusivo de la facultad y posibilitar la imposición de sanciones o la reparación del daño.

La relevancia fundamental del control judicial previo o inmediato de medidas de vigilancia encubierta que invaden la privacidad de las personas ha sido resaltada recientemente por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, la cual ha señalado que:

---

9 TEDH. *Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria.* Aplicación No. 62540/00. Sentencia de 28 de Junio de 2007; Caso *Weber y Sarabia vs. Alemania*. Aplicación No. 54934/00. Decisión de 29 de Junio de 2006.

10 Asamblea General de la Organización de las Naciones Unidas. Resolución A/RES/68/167 sobre el derecho a la privacidad en la era digital. 18 de Diciembre de 2013.

11 ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión Frank La Rue. 17 de abril de 2013. A/HRC/23/40.

12 OACNUDH. El derecho a la privacidad en la era digital. 30 de Junio de 2014. A/HRC/27/37

13 CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II.

14 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text

"Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover."[15]

En este sentido, la exigencia de que la solicitud se lleve a cabo con la debida fundamentación y motivación o el que se establezcan sanciones para aquellas autoridades que abusen de la facultad resultan ser medidas ilusorias que no inhiben los riesgos de abuso. Esto es así, en tanto el concesionario o autorizado no posee las herramientas para evaluar dicha fundamentación y motivación, sobre todo dada la vaguedad e imprecisión respecto de las circunstancias y el procedimiento para llevar a cabo la medida de vigilancia, y en cualquier caso se encuentra desincentivado a combatir dichas solicitudes dadas las graves sanciones de carácter administrativo e incluso penal que puede acarrear el incumplimiento de las solicitudes. En todo caso, la ausencia de control judicial previo o inmediato, aunada a la ausencia de otras salvaguardas, no permite la detección de abusos por parte de autoridades, ni permite la evaluación de la fundamentación y motivación de la solicitud por parte de una autoridad imparcial, independiente y especializada para ello, como lo es la autoridad judicial.

Resulta pertinente señalar que el control judicial previo o inmediato no impide necesariamente la efectividad de la medida de vigilancia o la celeridad necesaria para la consecución de fines legítimos, pues perfectamente pueden establecerse mecanismos de emergencia en los que la autorización judicial podría ser otorgada con efectos retroactivos de manera simultánea o posterior a que la autoridad válidamente lleve a cabo la medida, como fue propuesto en diversos momentos del proceso legislativo[16]. En este sentido, la efectividad o celeridad no pueden argumentarse como obstáculos inevitables para el control judicial, pues claramente existen formulaciones legales que concilian los objetivos de la medida de vigilancia y las salvaguardas necesarias al derecho a la privacidad de las personas.

Asimismo, no se contemplan en la Ley Federal de Telecomunicaciones y Radiodifusión o en otra legislación, medidas de supervisión independiente o de transparencia que funjan como contrapesos institucionales a las instancias que poseen facultades para invadir la privacidad de las

---

[15] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 165.

[16] Ver por ejemplo, Iniciativa con Proyecto de Decreto por el que se expide la Ley Federal de Telecomunicaciones y Radiodifusión. Gaceta del Senado. Primer periodo ordinario. Segundo año de ejercicio. LXII Legislatura. 28 de Octubre de 2013.

personas. Al respecto, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana ha señalado que *"los Estados deben establecer mecanismos de supervisión independientes sobre las autoridades encargadas de realizar las tareas de vigilancia"*[17]. En igual sentido, 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"[18] 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.*
>
> *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. (...)"*[19]

Otra de las salvaguardas fundamentales para proteger el derecho a la privacidad de los ciudadanos, garantizar el debido proceso y el acceso a un recurso efectivo que son ignoradas por la Ley Federal de Telecomunicaciones y Radiodifusión 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 fue interferida 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.

---

[17] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 170

[18] 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.

[19] 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

Este derecho de notificación a las personas afectadas por medidas de vigilancia han sido reconocidas, 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 respecto del uso de medidas de vigilancia de las comunicaciones"*[20]

(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.[21] No obstante, ni en la Ley Federal de Telecomunicaciones y Radiodifusión, ni en ninguna otra legislación aplicable, se contempla el derecho de notificación diferida a la persona afectada por una medida de vigilancia. Lo anterior no solamente constituye una violación al derecho a la privacidad, sino que además supone una vulneración al derecho a un debido proceso y a un recurso efectivo.

En efecto, como la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos lo han expresado:

> *"El artículo 8 de la Convención Americana no limita su aplicación a recursos judiciales sino que debe entenderse como el conjunto de requisitos que deben observarse en las instancias procesales a efecto de que las personas puedan defenderse adecuadamente ante cualquier tipo de acto emanado del Estado que pueda afectar sus derechos"*[22]

---

[20] 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

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

[22] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013.

En igual sentido, la ausencia del reconocimiento del derecho de notificación al afectado, aunado a la ausencia de control judicial o de supervisión independiente de las medidas de vigilancia como la localización geográfica, en tiempo real, de equipos de comunicación móvil, impiden al afectado tener conocimiento en algún momento de que el espacio de intimidad que protege el derecho a la privacidad ha sido interferido, y por tanto, se impide a la persona afectada el ejercicio del derecho a un recurso efectivo, conforme a las garantías del debido proceso.

En vista de lo anterior, debe concluirse que el artículo 190 fracción I de la Ley Federal de Telecomunicaciones y Radiodifusión debe ser declarado inconstitucional en tanto vulnera el derecho a la privacidad reconocido en los artículos 16 de la Constitución, 11.2 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos, así como los derechos a un debido proceso y a un recurso efectivo consagrados en los artículos 14, 16 y 17 de la Constitución, 8 y 25 de la Convención Americana sobre Derechos Humanos, 2.3 y 14 del Pacto Internacional de Derechos Civiles y Políticos.

El artículo 190 fracciones II y III de la Ley Federal de Telecomunicaciones y Radiodifusión viola los artículos 1, 14, 16 y 17 de la Constitución; los artículos 1.1, 2, 8.1 y 11.2 de la Convención Americana sobre Derechos Humanos; y los artículos 2.3, 14 y 17 del Pacto Internacional de Derechos Civiles y Políticos.

En el artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión se establecen obligaciones a los concesionarios de telecomunicaciones de conservar un registro y control de comunicaciones respecto de todas y todos sus usuarios, el cual incluye la conservación de datos, por 24 meses, sobre: el origen y destino de las comunicaciones; fecha, hora y duración de las comunicaciones; datos de identidad de los comunicantes; datos de identificación de los dispositivos; y datos de localización geográfica de los dispositivos. A su vez, la fracción III del propio artículo 190 ordena a los concesionarios y autorizados la entrega de los datos conservados, en los términos que a continuación se transcriben:

> ***"II.*** *Conservar un registro y control de comunicaciones que se realicen desde cualquier*

OEA/Ser.L/V/II, párr. 164; Corte IDH. Caso Ivcher Bronstein Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 6 de febrero de 2001. Serie C No. 74. Párr. 102; Corte IDH. Caso del Tribunal Constitucional Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 31 de enero de 2001. Serie C No. 55. Párr. 69; Corte IDH. Caso Baena Ricardo y otros Vs. Panamá. Fondo, Reparaciones y Costas. Sentencia de 2 de febrero de 2001. Serie C No. 72. Párr. 124.

tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

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

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

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

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

e) *Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;*

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

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

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

Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y

control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

III. *Entregar los datos conservados a las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables.*

Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente;"

La inconstitucionalidad de los artículos transcritos será demostrada de la siguiente manera:

1. La obligación de conservar de manera masiva e indiscriminada los datos a que se refiere el artículo 190 fracción II constituye una interferencia con el derecho a la privacidad, en concreto, con el derecho a la inviolabilidad de las comunicaciones privadas.

2. La obligación de conservación de datos establecida en el artículo 190 fracción II no constituye una restricción necesaria o proporcional y por tanto viola el derecho a la privacidad, en concreto a la inviolabilidad de las comunicaciones privadas.

3. El artículo 190 fracciones II y III viola el derecho a la privacidad al no cumplir con el requisito de previsión en la ley, pues no establece de manera clara, precisa y detallada las autoridades que pueden acceder a los datos conservados, las circunstancias en las que puede llevarse a cabo la medida, el procedimiento para el tratamiento, transmisión y destrucción de los datos obtenidos ni se establecen salvaguardas contra el abuso de las medidas, por lo que tampoco se cumple con el requisito de necesidad y proporcionalidad y se viola asimismo el debido proceso y el derecho a un recurso efectivo.

La conservación obligatoria e indiscriminada de los datos a que se refiere el artículo 190 fracción II, constituye una interferencia con el derecho a la privacidad, en

concreto, con el derecho a la inviolabilidad de las comunicaciones privadas.

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 de ejemplo, 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."*[23]

(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

[23] 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.

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 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 conforme 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.

El artículo 190 fracción II, viola el derecho a la privacidad, en concreto, a la inviolabilidad de las comunicaciones privadas reconocido en el artículo 16 constitucional, 11.2 de la Convención Americana sobre Derechos Humanos y 17 de Pacto Internacional de Derechos Civiles y Políticos en tanto la obligación de conservación indiscriminada de datos sobre las comunicaciones de la totalidad de las y los usuarios de telecomunicaciones no cumple con los requisitos de necesidad y proporcionalidad.

Como se ha señalado anteriormente, la conservación de datos que mandata el artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión se lleva a cabo de manera indiscriminada y masiva, es decir, respecto de todos los usuarios de servicios de telecomunicaciones, sin que exista indicio o circunstancia alguna que justifique la conservación y el tratamiento de los datos por un tiempo adicional al estrictamente necesario para la prestación del servicio.

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"*[24]

Asimismo, resulta determinante hacer referencia a la reciente decisión del Tribunal de Justicia

[24] 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

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[25]. 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 una plazo amplio de veinticuatro meses, sin que la conservación de datos por mayor tiempo del 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 constitucional confirman que la disposición analizada es violatoria del derecho a la inviolabilidad de las comunicaciones privadas.

Igualmente, la obligación de conservación de datos de comunicaciones, señalada en el artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión viola el artículo 16 constitucional, en concreto, el derecho de cancelación y oposición al tratamiento de datos personales en tanto anula el derecho a la autodeterminación informativa de manera arbitraria al impedir la revocación del consentimiento, que en su caso se otorgara, para que un particular, como lo son los concesionarios de telecomunicaciones y autorizados, recolectara, conservara e hiciera el tratamiento de datos personales, como lo son los señalados en el precepto analizado. Esto es así, en tanto el artículo 34 fracción IV de la Ley Federal de Protección de Datos en Posesión de Particulares en conjunción con el artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión impedirían el ejercicio del derecho de cancelación y oposición de manera arbitraria, en tanto, como ya ha sido argumentado, la obligación de conservación de datos no cumple con los requisito de necesidad y proporcionalidad. De esta forma, el artículo 190 fracción II, al no cumplir con el requisito de necesidad y proporcionalidad, interfiere de manera arbitraria e injustificada con el derecho de autodeterminación informativa.

Por lo tanto se concluye que el artículo 190 fracción II es inconstitucional al violar los artículos 16 constitucional, 11.2 de la Convención Americana sobre Derecho Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos.

---

[25] 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

El artículo 190 fracciones II y III, viola el derecho a la privacidad, en concreto, a la inviolabilidad de las comunicaciones privadas reconocido en el artículo 16 constitucional, 11.2 de la Convención Americana sobre Derechos Humanos y 17 de Pacto Internacional de Derechos Civiles y Políticos en tanto no cumple con el requisito de previsión en la ley. Asimismo, se incumple el requisito de necesidad y proporcionalidad, el debido proceso y el derecho a un recurso efectivo, reconocidos en los artículos 14, 16 y 17 de la Constitución, 8 y 25 de la Convención Americana sobre Derechos Humanos, 2.3 y 14 del Pacto Internacional de Derechos Civiles y Políticos.

El artículo 190 fracciones II y III establece la obligación de los concesionarios de telecomunicaciones de entregar los datos conservados a solicitud de diversas autoridades sin definirse de manera clara, precisa y detallada las autoridades que pueden acceder a los datos conservados, las circunstancias en las que puede llevarse a cabo la medida, el procedimiento para el tratamiento, transmisión y destrucción de los datos obtenidos, ni se establecen salvaguardas contra el abuso de las medidas, por lo tanto, dichos preceptos incumplen el requisito de previsión en la ley de las interferencias con el derecho a la privacidad, en concreto, a la inviolabilidad de las comunicaciones privadas.

Como se ha mencionado anteriormente, 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[26], 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.[27]

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

[26] *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.

[27] *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.

(...) 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."[28]

Igualmente, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos señaló recientemente que:

"Las normas legales vagas o ambiguas que otorgan facultades discrecionales muy amplias son incompatibles con la Convención Americana, porque pueden sustentar potenciales actos de arbitrariedad que se traduzcan en la violación del derecho a la privacidad o del derecho a la libertad de pensamiento y expresión garantizados por la Convención.

(...) Las leyes que habiliten la intercepción de las comunicaciones deben establecer con claridad y precisión las causas que el Estado puede invocar para solicitar esa intercepción, que sólo puede ser autorizada por un juez. Asimismo, se deben establecer por ley garantías vinculadas a la naturaleza, alcance y duración de las medidas de vigilancia; los hechos que podrían justificar esas medidas y las autoridades competentes para autorizarlas, llevarlas a cabo y supervisarlas. La ley debe ser clara en cuanto a posibles remedios para los abusos cometidos en el ejercicio de esas facultades."[29]

En el caso del artículo 190 fracciones II y III, no se señalan con precisión las autoridades facultadas para solicitar el acceso a datos conservados por los concesionarios de telecomunicaciones, pues únicamente se hace referencia a las autoridades que menciona el artículo 189 de la Ley, el cual incluye a las "instancias de seguridad", las cuales, como ha sido señalado anteriormente, no se encuentran definidas por esta ley, ni por otras disposiciones aplicables. De esta forma se confirma la inconstitucionalidad de dichas disposiciones.

De igual manera, ni la Ley Federal de Telecomunicaciones y Radiodifusión, ni otra legislación aplicable, establecen con precisión las circunstancias en las que esta severa interferencia con el derecho a la privacidad podría estar justificada. Como fue señalado, por ejemplo, por el Tribunal de Justicia de la Unión Europea, la indefinición precisa de los delitos bajo investigación que justificarían

---

[28] 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.

[29] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II.

el acceso a datos conservados produce la violación del derecho a la privacidad. En el caso de las "instancias de seguridad", resultan aún más indefinidas y por ende, arbitrarias, las circunstancias en las que dichas autoridades podrían acceder a los datos conservados.

Por su parte, la fracción II del artículo 190 establece que los concesionarios deberán poner a disposición los datos conservados "*en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos".* Asimismo, la fracción III de dicho artículo obliga a los concesionarios a entregar los datos conservados a través de la mera solicitud por parte de las autoridades, sin establecer de manera explícita la necesidad de la autorización judicial federal, según lo establece el artículo 16 constitucional.

La relevancia fundamental del control judicial previo de medidas de vigilancia de comunicaciones ha sido resaltada recientemente por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, la cual ha señalado que:

> *"Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover."*[30]

En este sentido, la exigencia de que la solicitud se lleve a cabo con la debida fundamentación y motivación o el que se establezcan sanciones para aquellas autoridades que abusen de la facultad resultan ser medidas ilusorias que no inhiben los riesgos de abuso. Esto es así, en tanto el concesionario o autorizado no posee las herramientas para evaluar dicha fundamentación y motivación, sobre todo dada la vaguedad e imprecisión respecto de las circunstancias y el procedimiento para llevar a cabo la medida de vigilancia, y en cualquier caso se encuentra desincentivado a combatir dichas solicitudes dadas las graves sanciones de carácter administrativo e incluso penal que puede acarrear el incumplimiento de las solicitudes. En todo caso, la ausencia de control judicial previo, aunada a la ausencia de otras salvaguardas, no permite la detección de abusos por parte de autoridades, ni permite la evaluación de la fundamentación y motivación de la solicitud por parte de una autoridad imparcial, independiente y especializada para ello, como lo es la autoridad judicial.

---

[30] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 165.

Resulta pertinente señalar que el control judicial previo no impide necesariamente la efectividad de la medida de vigilancia o la celeridad necesaria para la consecución de fines legítimos, pues perfectamente pueden establecerse mecanismos de emergencia en los que la autorización judicial podría ser otorgada con efectos retroactivos de manera simultánea o posterior a que la autoridad válidamente lleve a cabo la medida, como fue propuesto en diversos momentos del proceso legislativo[31]. En este sentido, la efectividad o celeridad no pueden argumentarse como obstáculos inevitables para el control judicial, pues claramente existen formulaciones legales que concilian los objetivos de la medida de vigilancia y las salvaguardas necesarias al derecho a la privacidad de las personas.

Asimismo, no se contemplan en la Ley Federal de Telecomunicaciones y Radiodifusión o en otra legislación, medidas de supervisión independiente o de transparencia que funjan como contrapesos institucionales a las instancias que poseen facultades para invadir la privacidad de las personas. Al respecto, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana ha señalado que *"los Estados deben establecer mecanismos de supervisión independientes sobre las autoridades encargadas de realizar las tareas de vigilancia"*[32]. En igual sentido, 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"[33] 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.*

---

31 Ver por ejemplo, Iniciativa con Proyecto de Decreto por el que se expide la Ley Federal de Telecomunicaciones y Radiodifusión. Gaceta del Senado. Primer periodo ordinario. Segundo año de ejercicio. LXII Legislatura. 28 de Octubre de 2013.

32 CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 170.

33 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. (...)"[34]

Otra de las salvaguardas fundamentales para proteger el derecho a la privacidad de los ciudadanos, garantizar el debido proceso y el acceso a un recurso efectivo que son ignoradas por la Ley Federal de Telecomunicaciones y Radiodifusión 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 fue interferida 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 han sido reconocidas, 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 respecto del uso de medidas de vigilancia de las comunicaciones"*[35]

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.[36] No obstante, ni en la Ley Federal de Telecomunicaciones y Radiodifusión, ni en ninguna

---

[34] 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

[35] 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

[36] TEDH. *Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria.*

otra legislación aplicable, se contempla el derecho de notificación diferida a la persona respecto de la cual los datos de sus comunicaciones han sido accesados. Lo anterior no solamente constituye una violación al derecho a la privacidad, sino que además supone una vulneración al derecho a un debido proceso y a un recurso efectivo.

En efecto, como la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos lo han expresado:

> *"El artículo 8 de la Convención Americana no limita su aplicación a recursos judiciales sino que debe entenderse como el conjunto de requisitos que deben observarse en las instancias procesales a efecto de que las personas puedan defenderse adecuadamente ante cualquier tipo de acto emanado del Estado que pueda afectar sus derechos"*[37]

En igual sentido, la ausencia del reconocimiento del derecho de notificación al afectado, aunado a la ausencia de control judicial o de supervisión independiente de las medidas de vigilancia de comunicaciones, como el acceso a datos que identifican las comunicaciones de una persona, impiden al afectado tener conocimiento en algún momento de que el espacio de intimidad que protege el derecho a la privacidad y a la inviolabilidad de las comunicaciones privadas ha sido interferido, y por tanto, se impide a la persona afectada el ejercicio del derecho a un recurso efectivo, conforme a las garantías del debido proceso.

En vista de lo anterior, debe concluirse que el artículo 190 fracción II y III de la Ley Federal de Telecomunicaciones y Radiodifusión debe ser declarado inconstitucional en tanto vulnera el derecho a la privacidad reconocido en los artículos 16 de la Constitución, 11.2 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos, así como los derechos a un debido proceso y a un recurso efectivo consagrados en los artículos 14, 16 y 17 de la Constitución, 8 y 25 de la Convención Americana sobre Derechos Humanos, 2.3 y 14 del Pacto Internacional de Derechos Civiles y Políticos.

Aplicación No. 62540/00. Sentencia de 28 de Junio de 2007

[37] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 164; Corte IDH. Caso Ivcher Bronstein Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 6 de febrero de 2001. Serie C No. 74. Párr. 102; Corte IDH. Caso del Tribunal Constitucional Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 31 de enero de 2001. Serie C No. 55. Párr. 69; Corte IDH. Caso Baena Ricardo y otros Vs. Panamá. Fondo, Reparaciones y Costas. Sentencia de 2 de febrero de 2001. Serie C No. 72. Párr. 124.