INSTITUTO FEDERAL DE TELECOMUNICACIONES

Instituto Federal de Telecomunicaciones
029.
12 ENE. 2016
RECIBIDO
AREA OTP
NOMBRE Y HORA Ivan 18:12

**OFICINA COMISIONADA**
**IFT/100/PLENO/OC-ASLI/02/2016**

México, D.F., a 12 de enero de 2016

**LIC. JUAN JOSÉ CRISPÍN BORBOLLA**
**SECRETARIO TÉCNICO DEL PLENO**
**Presente**

Por este medio envío a usted, para los efectos conducentes, el engrose del voto particular disidente que formulé oralmente durante la XLIII Sesión Extraordinaria del Pleno del Instituto Federal de Telecomunicaciones, celebrada el 11 de noviembre de 2015, respecto al "ACUERDO MEDIANTE EL CUAL EL PLENO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES EXPIDE LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA Y MODIFICA EL PLAN TÉCNICO FUNDAMENTAL DE NUMERACIÓN PUBLICADO EN EL DOF EL 21 DE JUNIO DE 1996". Esta Resolución fue aprobada por el Pleno, mediante Acuerdo P/IFT/EXT/111115/159.

**Atentamente,**

**ADRIANA SOFÍA LABARDINI INZUNZA**
**COMISIONADA DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES**

**VOTO PARTICULAR SOBRE EL ASUNTO ENLISTADO BAJO EL NUMERAL III.1 DE LA ORDEN DEL DIA DE LA XLIII SESIÓN EXTRAORDINARIA, DENOMINADO "ACUERDO MEDIANTE EL CUAL EL PLENO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES EXPIDE LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA Y MODIFICA EL PLAN TÉCNICO FUNDAMENTAL DE NUMERACIÓN PUBLICADO EN EL DOF EL 21 DE JUNIO DE 1996".**

## INTRODUCCIÓN

El presente voto es el resultado de un largo y cuidadoso análisis del "*Acuerdo Mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia, y Modifica el Plan Técnico Fundamental de Numeración*" que se presentó a nuestra consideración (en adelante, el "Proyecto de Lineamientos" o los "Lineamientos") así como de la revisión de: i) los comentarios vertidos en la consulta pública respectiva, ii) el análisis de impacto regulatorio; y iii) el seguimiento de actas levantadas y reuniones formales con autoridades de seguridad y justicia, agentes regulados y autorizados del sector de telecomunicaciones, así como de diversas asociaciones civiles especializadas en el tema, asociaciones de víctimas de la delincuencia y cámaras de la industria de las telecomunicaciones que expresaron sus puntos de vista sobre el Proyecto.

La Ley Federal de Telecomunicaciones y Radiodifusión (en adelante, la "LFTR") faculta al Instituto Federal de Telecomunicaciones (en lo sucesivo, el "Instituto") a emitir los Lineamientos en materia de Colaboración con la Justicia, según lo dispuesto en sus artículos 189 y 190. Si dicha facultad legal excede o no el mandato constitucional del Instituto, es algo que el Pleno no puede resolver y que decidió, en su momento no someter a la decisión de la Suprema Corte de Justicia a través de una controversia constitucional. Por ende, el Instituto está obligado a aplicar la LFTR y por ende a expedir los Lineamientos.

Tal obligación no implica que el Pleno no pueda interpretar la LFTR, en específico, los artículos 189 y190, en los términos del artículo 1° constitucional, a fin de que con la emisión de éstos, promovamos, respetemos, protejamos y garanticemos los derechos humanos. Por lo mismo, es necesario que hagamos una interpretación conforme con la Constitución Política de los Estados Unidos Mexicanos y con los tratados internacionales de la materia, bajo los principios de universalidad, interdependencia, indivisibilidad y progresividad.

Así, ante esta delicada tarea que el Poder Legislativo nos encomienda, considero que existen tres condiciones imprescindibles que el Instituto debe seguir:

1. Que se establezcan reglas, mecanismos, procedimientos y procesos en los Lineamientos, que permitan una clara, efectiva y oportuna colaboración con la justicia.

2. Que los Lineamientos respeten los derechos humanos reconocidos en nuestra Constitución y en los tratados internacionales de los que México es parte. Los requerimientos de geolocalización en tiempo real, intervención de las comunicaciones (a fin de escuchar, grabar o acceder al contenido de las comunicaciones de las personas), y el acceso al registro de datos (que de *iure* es también una intervención de comunicaciones) deben tener el único objeto de salvaguardar bienes jurídicamente tutelados, como la seguridad pública y nacional. No obstante dichos actos constituyen restricciones a otros derechos humanos (en especial, al de privacidad y al de libertad de expresión).

   Por ello es necesario que estas restricciones a derechos humanos se acoten a lo mínimo indispensable a lo largo de los Lineamientos y del sistema que éstos creen e implementen. Esto de acuerdo a los principios de legalidad, debido proceso, necesidad, urgencia, proporcionalidad, transparencia y rendición de cuentas. Así lo ha resuelto la Suprema Corte de Justicia de la Nación en el caso de la localización geográfica; la Corte Interamericana de Derechos Humanos y la Comisión Interamericana de Derechos Humanos como más adelante se abordará.

3. Que se geste un ecosistema integral de colaboración (que incluye los Lineamientos, sus anexos, los sistemas a ser implementados, los protocolos de seguridad, los accesos a la plataforma, la gobernanza y actos de los Grupos de Trabajo, las autoridades facultadas y los concesionarios y autorizados) capaz de salvaguardar desde su diseño y en forma efectiva, la protección de la privacidad y los datos personales de los usuarios y los demás derechos protegidos por la Constitución y los tratados internacionales. El Instituto tiene la enorme responsabilidad de evitar que se geste otro engendro como el del RENAUT, que mal diseñado, mal implementado y mal supervisado, resultó en que esa gigantesca y sensible base de datos personales se comercializara ilegalmente en el mercado negro y, por otro lado, no logró su objetivo de coadyuvar en la investigación, prevención y persecución de delitos

La metodología empleada por la Unidad de Política Regulatoria, responsable de elaborar los Lineamientos se basó en escuchar a todas las partes afectadas y lo hizo a cabalidad. Los Comisionados también escuchamos a autoridades, industria, organizaciones de la sociedad civil y ciudadanos. Sin embargo, debió también escuchar a expertos independientes en procesos de inteligencia; logística y hacer análisis propios de tipo

jurídico constitucional; de gestión de riesgos, y de alternativas de gobernanza del sistema de colaboración, pues la responsabilidad del Instituto no se agota con la emisión de Lineamientos sino que deberá garantizar, según una interpretación conforme, los requisitos a que me he referido para poder dar por cumplido su mandato conforme a los artículos 189 y 190. Su trabajo fue titánico y loable, pero los Lineamientos, desafortunadamente, no parecen dar génesis a un sistema logísticamente robusto, confiable, seguro, jurídicamente sostenible y operativamente eficaz.

Considero que el Instituto debe establecer no sólo obligaciones y cargas a sus regulados, sino detonar un sistema capaz de proteger a los usuarios limitando a lo estrictamente necesario, proporcional y con herramientas que en forma efectiva salvaguarden los datos personales en poder de autoridades y de concesionarios por igual. De este modo, unos Lineamientos que solamente crean cargas para los Concesionarios y Autorizados pero que no obligan a las Autoridades Facultadas a utilizar y resguardar un sistema o plataforma única con procesos y protocolos de seguridad estrictos y precisos de implementación certificada; y que por el contrario permite sistemas alternativos u opcionales para las autoridades para requerir y recibir la información requerida, por distintas vías, con diversos protocolos y grupos de trabajo *adhoc* y de alcances demasiado amplios, no puede ser un sistema efectivo ni seguro.[1]

Asimismo, el Proyecto de Lineamientos encarga a los regulados, siendo empresas privadas, la tarea de calificar y decidir si el requerimiento es procedente, legal, justificado, y proveniente de una autoridad facultada, con lo que el Instituto claudica a su misión de tutelar derechos de los usuarios y los derechos a la protección de los datos personales-aunque esto sea en forma indirecta-. De este modo a través de los Lineamientos no se establece un sistema de gestión y gobernanza robusto y efectivo.

Según datos de ANATEL, en el año 2013 sus socios recibieron requerimientos por oficio, de autoridades federales, locales y municipales para investigar decenas de miles de líneas telefónicas requeridas a través de numerosos oficios. La precaria situación de seguridad e impunidad en el país y el incipiente sistema acusatorio de justicia penal, exigen un sistema moderno, robusto, seguro y eficaz, cuya construcción sólo es posible mediante sofisticadas plataformas y procesos informáticos de inteligencia y con la intervención de un juez de control en el caso de, por ejemplo, el acceso al registro de datos sobre el uso de líneas telefónicas, léase voz y mensajes de texto (no aplicaciones usadas a partir del número telefónico).

[1] Ver diagrama de flujo de elaboración propia a partir de los datos y procesos insertos en los Lineamientos que revela incertidumbre en una serie de decisiones a tomar por Concesionarios, Autorizados y las propias Autoridades.

Por lo anteriormente expuesto, considero que el IFT tiene el deber de ser exhaustivo en el diseño e implementación de estos procesos de colaboración a fin de que la merma en privacidad que los usuarios de telecomunicaciones podrán sufrir, y las inversiones y gastos de operación que se requerirán -y que debe quedar claro quienes las asumirán-, se vean compensados por lo menos con el abatimiento de la impunidad, con mejores resultados en la prevención, investigación y persecución de conductas delictuosas, salvaguardando eficazmente los derechos humanos de los usuarios afectados.

Para ello el Instituto no puede evadir un rol central de coordinación y supervisión de la gestión, a través de sus facultades explícitas e implícitas a fin de que sus Lineamientos logren una colaboración efectiva y oportuna, pero respetuosa de límites. Para ello no puede ni delegar a los particulares funciones de Estado, ni dejar intocadas a las Autoridades que requieren de la colaboración y quienes también deben tener claras obligaciones, límites y quedar sujetos a procesos, protocolos ciertos, dentro de los Lineamientos y en la implementación del sistema colaborativo. Es decir, el actuar del Instituto tiene que centrarse en crear un clima y ambiente controlado de colaboración efectiva y oportuna que sea respetuosa de todos los derechos que se encuentran en juego.

Una vez expuesto lo anterior, procedo a manifestar y engrosar las razones por las que, si bien voté a favor en lo general del Proyecto de Lineamientos, no obstante me aparté de ciertos artículos. Para efectos prácticos, el presente voto se divide en tres apartados. En el primero expongo brevemente el marco jurídico en materia de derechos humanos y de derecho comparado, así como buenas prácticas internacionales que sirven como marco de referencia para analizar los presentes Lineamientos. En el apartado segundo realizo un análisis de los principales problemas que he identificado respecto a los Lineamientos y expongo las razones por las que considero que son incompatibles con el marco referido en el primer apartado. Por último, en el tercer apartado menciono las cuestiones que ameritaron un voto diferenciado de mi parte. Es decir, una vez expuesta mi posición respecto a los principales problemas y teniendo en cuenta los argumentos ahí señalados, referiré los considerandos, artículos, capítulos y anexos del Proyecto que no comparto.

## 1. Marco jurídico en materia de Derechos Humanos

En lo que respecta a este marco hay que identificar, por lo menos, tres rubros relevantes. En primer lugar, el marco constitucional y los derechos humanos que se encuentran en juego; en segundo lugar, los criterios orientadores sobre geolocalización e intervención de comunicaciones que ha emitido la Suprema Corte de Justicia de la Nación y, en tercer lugar, los criterios sobre el alcance de la interpretación conforme, el principio *pro persona* y el control difuso, lo que nos llevará a crear un nuevo marco interpretativo en materia de derechos humanos.

## 1.1. Marco nacional

### 1.1.1. Marco constitucional

Respecto al primer aspecto, el marco constitucional que debemos tomar en cuenta para la expedición de los Lineamientos se compone de los derechos que pueden verse vulnerados o afectados como consecuencia del mandato legal de emitir los Lineamientos y en las facultades explícitas e implícitas que tiene el Instituto para proteger estos derechos. De esta manera, los derechos, por un lado, tienen que ser ponderados y, por otro, tomarse en cuenta al regular o crear políticas públicas en la materia. A continuación se exponen los artículos constitucionales más relevantes en para efectos del análisis del presente Proyecto.

El artículo 1° constitucional, como se mencionó anteriormente, reconoce la obligación de todas las autoridades, en el ámbito de sus competencias, de promover, respetar, proteger y garantizar los derechos humanos. De la misma manera, establece que las normas relativas a los derechos humanos se interpretarán de conformidad con la Constitución y con los tratados internacionales de la materia. Dicho numeral es, sin duda, uno de los sustentos más importantes de la obligación que tiene el Instituto de hacer un análisis mucho más amplio y elevar el estándar de protección; dado que, el IFT, al ser una autoridad, no puede obviar su tarea de proteger los derechos humanos que le han sido encomendados.

Bajo la premisa de que el Instituto es una autoridad encargada de promover, respetar, proteger y garantizar los derechos humanos, y una vez estudiado el ámbito de sus competencias, podemos observar que es de especial relevancia proteger los derechos a la libertad de expresión y a la información consagrados en los artículos 6° y 7° constitucionales. Esto, ya que, según el artículo 28 constitucional, el Instituto tiene como mandato garantizar lo dispuesto en dichos numerales. Por lo mismo, de ellos se derivan ciertas facultades que tienen que ser compatibles con los mecanismos que se establecerán en los Lineamientos. Es decir, es necesario analizar y ponderar de qué manera los Lineamientos pueden influir o incidir en la correcta garantía y protección de la libertad de expresión y el derecho a acceso a la información, dado que su protección es parte de una facultad directa que tiene el Instituto.

De la misma manera, por la naturaleza de los Lineamientos, se vuelven muy relevantes los artículos 14 y 16 constitucionales. El artículo 16 consagra el derecho a la inviolabilidad de las comunicaciones privadas, derecho que se encuentra reconocido plena y autónomamente en la Constitución como parte de aquellos derechos que preservan al individuo de un ámbito libre de injerencias de terceros. Por lo mismo, para la emisión de

los lineamientos era necesario hacer un análisis minucioso sobre los alcances de su contenido y el objeto de su protección. Asimismo, era necesario establecer, con base en criterios nacionales e internacionales, en qué momento se consuma la violación a este derecho y qué estándares tienen que tomarse en cuenta para su protección, como lo estudiaré más adelante en el apartado segundo.

Del mismo modo, de acuerdo con los artículos 14, segundo párrafo, y 16, primer párrafo, de la Constitución, una persona no puede ser privada de sus derechos si no es mediante juicio seguido ante Tribunales competentes, ni ser molestada en su persona sin mandamiento escrito fundado y motivado, por parte de la autoridad competente. Esto tenía que ser ponderado, de la misma manera, en nuestro análisis, ya que establece un estándar para efectuar actos de molestia, como podrían ser los previstos en los Lineamientos.

Otro derecho que, por supuesto, tiene que valorarse es el derecho que tienen los individuos a la seguridad. Se considera muy relevante tomar en cuenta este derecho ya que responde directamente a uno de los fines en los que se basan los artículos 189 y 190 de la LFTR. Así las cosas, en la ponderación correspondiente es necesario establecer un estándar claro sobre de qué manera y con qué controles se hará valer este derecho en concordancia con los artículos anteriormente mencionados. Pero, de la misma manera, los Lineamientos tendrían que establecer controles eficaces para poder proteger este derecho de la mejor manera posible.

### 1.1.2. Criterios relevantes de la Suprema Corte de Justicia de la Nación sobre la inviolabilidad de las comunicaciones privadas

Algunos de los derechos anteriormente mencionados ya han sido interpretados por la Suprema Corte de Justicia de la Nación (en adelante, la "SCJN"). Esto es relevante ya que, a pesar de que los criterios emitidos por la misma no nos obligan de manera directa, sirven como criterios orientadores sobre el contenido de los derechos antes mencionados. Asimismo, para poder protegerlos de manera satisfactoria es necesario preguntarnos cuál es el estándar de protección que se ha establecido tanto nacional como internacionalmente.

La SCJN se ha pronunciado respecto a la necesidad de proteger las comunicaciones privadas, estableciendo ciertos límites y estándares que tienen que servir como guía al Instituto para la elaboración de los Lineamientos. Los criterios y las partes relevantes de los mismos se encuentran a continuación:

**DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SUS DIFERENCIAS CON EL DERECHO A LA INTIMIDAD.**[2] 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.

Según el criterio antes transcrito, el derecho a la inviolabilidad de las comunicaciones se configura como una garantía formal. Para ésta tesis, lo que se encuentra prohibido por el artículo 16 constitucional es la intercepción, el registro o el conocimiento antijurídico de una comunicación ajena con independencia de su contenido y de la difusión de este contenido. Es decir, 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.

**DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE IDENTIFICAN LA**

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

> **COMUNICACIÓN.**[3] 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.**

Aunado a lo anterior, el objeto de protección constitucional del derecho a la inviolabilidad de las comunicaciones privadas hace referencia también a aquellos datos que identifican la comunicación o de datos externos a la comunicación. Según este criterio, 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.

> **COMUNICACIONES PRIVADAS. EL DERECHO A SU INVIOLABILIDAD, CONSAGRADO EN EL ARTÍCULO 16, PÁRRAFO NOVENO, DE LA CONSTITUCIÓN FEDERAL, ES OPONIBLE TANTO A LAS AUTORIDADES COMO A LOS GOBERNADOS, QUIENES AL TRANSGREDIR ESTA PRERROGATIVA**

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

> **INCURREN EN LA COMISIÓN DE UN ILÍCITO CONSTITUCIONAL.**[4] Del análisis de lo dispuesto en diversos preceptos de la Constitución Política de los Estados Unidos Mexicanos, se advierte que la misma contiene mandatos cuyos destinatarios no son las autoridades, sino que establece deberes a cargo de los gobernados, como sucede, entre otros casos, de lo dispuesto en sus artículos 2o., 4o. y 27, en los que la prohibición de la esclavitud, el deber de los padres de preservar el derecho de los menores a la satisfacción de sus necesidades y a la salud física y mental, así como los límites a la propiedad privada, constituyen actos u omisiones que deben observar aquéllos, con independencia de que el mandato constitucional constituya una garantía exigible a las autoridades y que, por ende, dentro de su marco competencial éstas se encuentren vinculadas a su acatamiento. En tal virtud, **al establecer el Poder Revisor de la Constitución**, en el párrafo noveno del artículo 16 de la Constitución General de la República, que las "comunicaciones privadas son inviolables", **resulta inconcuso que con ello estableció como derecho fundamental el que ni la autoridad ni los gobernados pueden intervenir una comunicación, salvo en los casos y con las condiciones que respecto a las autoridades establece el propio numeral** y, por tanto, la infracción de los gobernados a tal deber conlleva la comisión de un ilícito constitucional, con independencia de los efectos que provoque o del medio de defensa que se prevea para su resarcimiento, en términos de la legislación ordinaria correspondiente.

Del criterio anterior, se desprende que ni la autoridad ni los gobernados pueden intervenir una comunicación, salvo en los casos y con las condiciones que respecto a las autoridades establece el artículo 16 constitucional.

Los criterios judiciales anteriormente mencionados crearon un estándar claro sobre qué se entiende como intervención de comunicaciones y qué es lo que se tiene que proteger y por ello deben guiar al Instituto en la elaboración de los Lineamientos.

### 1.1.3. Criterios de la SCJN sobre Geolocalización: *acción de inconstitucionalidad 32/2012*

Los criterios anteriormente mencionados responden, específicamente, a la intervención de comunicaciones. Sin embargo, respecto a los criterios que regulan la geolocalización, es

[4] Época: Novena Época. Registro: 190652. Instancia: Segunda Sala. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XII, Diciembre de 2000 Materia(s): Constitucional. Tesis: 2a. CLX/2000. Página: 428. Amparo en revisión 2/2000. Norma Angélica Medrano Saavedra. 11 de octubre del año 2000. Unanimidad de cuatro votos. Ausente: José Vicente Aguinaco Alemán. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: María Elena Rosas López.

importante remitirnos al precedente más reciente de la SCJN, que es la acción de inconstitucionalidad 32/2012.

El promovente de esta acción fue la Comisión Nacional de los Derechos Humanos para declarar inválidos los artículos 133 Quáter, del Código Federal de Procedimientos Penales y 16, fracción I, apartado D y 40 Bis de la Ley Federal de Telecomunicaciones.

Según la ejecutoria, la medida de Geolocalización se constriñe al objeto de conocer el lugar aproximado desde el cual se origina una llamada proveniente de un teléfono móvil, asociado a una línea determinada o identificada y procede **sólo en caso de que los equipos móviles, asociados a una línea, se encuentren relacionados en las investigaciones de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas.**

Desde esta perspectiva, por la protección al orden público y la paz social, así como la tutela a los derechos de la vida e integridad física y psicológica de las personas se justifica esta medida. No obstante, se ha precisado que se acota a la ubicación del lugar del que proviene una llamada realizada a través de un equipo móvil asociado a una línea y no comprende la intervención de comunicaciones, ni el registro de llamadas, medidas para las cuales, según la Suprema Corte, existe una diversa reglamentación.

Esto quiere decir que su ejercicio no procede indiscriminadamente, sino únicamente en aquellos casos en que se cuente con elementos suficientes que hagan probable la comisión de los delitos que taxativamente enumeran las normas impugnadas, todos ellos de gravedad o particular trascendencia. También, la Corte aclaró que se trataba de casos de tal magnitud que el ejercicio de la medida es de urgente necesidad, bien porque se encuentra en riesgo la vida o integridad física de las víctimas del delito, o bien, existe peligro de que se oculte o desaparezca el objeto o instrumentos del ilícito.

Por lo mismo, las normas impugnadas son constitucionales *si y sólo si,* se interpreta que las mismas tienen aplicación únicamente en estos supuestos de excepción, lo cual deberá estar suficientemente motivado por la autoridad competente.

Conviene señalar que la explicable necesidad de que en algunos casos la geolocalización deba dictarse con la premura requerida para proteger a las víctimas o preservar la identificación del lugar en que se origina una llamada, tampoco releva a la autoridad ministerial de su obligación constitucional de fundar y motivar sus actos, concretamente mediante: *1. La instrucción al personal técnico que corresponda, que mínimamente razone la excepcionalidad del caso, dado el tipo de delitos que se investiga; 2. La averiguación previa en la que se provee la medida, y 3. Las condiciones fácticas que revelen la eventualidad de daño a las personas o del ocultamiento de datos para esclarecer los*

*hechos de la investigación*; de todo lo cual habrá de dejarse constancia en el expediente cuya información deberá de mantenerse en sigilo hasta el momento procesal oportuno, de modo que ni aún el concesionario o permisionario del servicio puedan acceder a ella.

Como se observa, la geolocalización no procede en todos los casos y el estándar tiene que estar claramente determinado para que respete los principios antes mencionados. El siguiente cuadro, representa y esquematiza el estándar propuesto por la Suprema Corte.

| Tabla 1.- Geolocalización | | | |
|---|---|---|---|
| **¿Cuándo procede esta facultad?** | **¿Cuáles son los elementos relevantes que deben contemplarse en la fundamentación y motivación de la medida?** | **¿Cómo debe solicitarse?** | **Temporalidad** |
| Únicamente en aquellos casos en que se cuente con elementos suficientes que hagan probable la comisión de los delitos que taxativamente se enuncian. | La instrucción al personal técnico que corresponda, que mínimamente razone la excepcionalidad del caso, dado el tipo de delitos que se investiga. | Constar por escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. | Mientras subsista el hecho que la originó, y colmado éste, tal facultad se extingue. |
| Casos de tal magnitud que el ejercicio de la medida es de urgente necesidad. | La averiguación previa en la que se provee la medida. | Sólo la podrá requerir en los supuestos que acota la disposición, extremos que en todos los casos deben cumplirse. | |
| Las normas impugnadas son constitucionales si y sólo si, se interpreta que las mismas tienen aplicación únicamente en | Las condiciones fácticas que revelen la eventualidad de daño a las personas o del ocultamiento de datos para esclarecer los | Dejar constancia en autos de la solicitud. | |

| | | | |
|---|---|---|---|
| estos supuestos de excepción, lo cual deberá estar suficientemente motivado por la autoridad competente. | hechos de la investigación. | | |

**1.1.4. Los criterios sobre el alcance de la interpretación conforme, el control difuso y la aplicabilidad del derecho internacional en nuestro sistema normativo**

Para poder aplicar y entender los criterios presentados con anterioridad, es necesario tener un parámetro analítico e interpretativo que nos permita ponderar y saber en qué momento estamos frente a una restricción válida y en qué momento aplicar un derecho sobre otro. Para eso, es importante notar que en la actualidad, vivimos un nuevo paradigma de control e interpretación constitucional. Al efecto, la SCJN ya indicó que, conforme al artículo 1º constitucional, párrafo tercero, es obligación de todas las autoridades respetar, proteger, promover y garantizar los derechos humanos, para ello el primer paso es interpretar las leyes con un sentido que se ajuste a lo dispuesto por tales derechos y otras prescripciones de superior jerarquía[5]. Asimismo, el segundo párrafo del artículo 1o. constitucional prevé un mandato imperativo en materia de derechos humanos (es decir, no deja a potestad de los poderes su aplicación, sino que impone un mandato de oficio a éstos).

Este mandato oficioso, del que deriva la obligatoriedad en nuestro país de aplicar y ceñirnos a este nuevo paradigma de control, no sólo surge de la reforma constitucional en materia de derechos humanos, vigente desde el 11 de junio de 2011, sino que también tiene como fundamento las siguientes fuentes de derecho:

**CONVENCION AMERICANA SOBRE DERECHOS HUMANOS (Pacto de San José) (vigente en nuestro país desde 24 de marzo de 1981)**

> ***Artículo 1. Obligación de Respetar los Derechos***
> *1. Los Estados Partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opiniones políticas o*

[5] Ferrer Mac Gregor, *Eduardo, Interpretación conforme y control difuso de convencionalidad. El nuevo paradigma para el juez mexicano*. Instituto de Investigaciones Jurídicas UNAM, México.

*de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social.*
*2. Para los efectos de esta Convención, persona es todo ser humano.*

***Artículo 2. Deber de Adoptar Disposiciones de Derecho Interno***
*Si el ejercicio de los derechos y libertades mencionados en el artículo 1 no estuviere ya garantizado por disposiciones legislativas o de otro carácter, los Estados Partes se comprometen a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones de esta Convención, las medidas legislativas o de otro carácter que fueren necesarias para hacer efectivos tales derechos y libertades.*

***Artículo 29. Normas de Interpretación***
*Ninguna disposición de la presente Convención puede ser interpretada en el sentido de:*
*a) permitir a alguno de los Estados Partes, grupo o persona, suprimir el goce y ejercicio de los derechos y libertades reconocidos en la Convención o limitarlos en mayor medida que la prevista en ella;*
*b) limitar el goce y ejercicio de cualquier derecho o libertad que pueda estar reconocido de acuerdo con las leyes de cualquiera de los Estados Partes o de acuerdo con otra convención en que sea parte uno de dichos Estados;*
*c) excluir otros derechos y garantías que son inherentes al ser humano o que se derivan de la forma democrática representativa de gobierno, y*
*d) excluir o limitar el efecto que puedan producir la Declaración Americana de Derechos y Deberes del Hombre y otros actos internacionales de la misma naturaleza.*

**Convención de Viena sobre el derecho de los tratados (vigente en nuestro país desde el 27 de enero de 1980)[6]**

***Artículo 26.***
*"Pacta sunt servanda". Todo tratado en vigor obliga a las partes y debe ser cumplido por ellas de buena fe.*

***Artículo 27.***
*El derecho interno y la observancia de los tratados. Una parte no podrá invocar las disposiciones de su derecho interno como justificación del incumplimiento*

*de un tratado. Esta norma se entenderá sin perjuicio de lo dispuesto en el artículo 46.*

**Caso Gelman vs. Uruguay, sentencia de 24 de febrero de 2011, párrafo 239.**

***Párrafo 239.*** *La sola existencia de un régimen democrático no garantiza, per se, el permanente respeto del Derecho Internacional, incluyendo al Derecho Internacional de los Derechos Humanos, lo cual ha sido así considerado incluso por la propia Carta Democrática Interamericana. La legitimación democrática de determinados hechos o actos en una sociedad está limitada por las normas y obligaciones internacionales de protección de los derechos humanos reconocidos en tratados como la Convención Americana, de modo que la existencia de un verdadero régimen democrático está determinada por sus características tanto formales como sustanciales, por lo que, particularmente en casos de graves violaciones a las normas del Derecho Internacional de los Derechos,* ***la protección de los derechos humanos constituye un límite infranqueable a la regla de mayorías, es decir, a la esfera de lo "susceptible de ser decidido" por parte de las mayorías en instancias democráticas, en las cuales también debe primar un "control de convencionalidad" (supra párr. 193), que es función y tarea de cualquier autoridad pública y no sólo del Poder Judicial.*** *En este sentido, la Suprema Corte de Justicia ha ejercido, en el Caso Nibia Sabalsagaray Curutchet, un adecuado control de convencionalidad respecto de la Ley de Caducidad, al establecer, inter alia, que "el límite de la decisión de la mayoría reside, esencialmente, en dos cosas: la tutela de los derechos fundamentales (los primeros, entre todos, son el derecho a la vida y a la libertad personal, y no hay voluntad de la mayoría, ni interés general ni bien común o público en aras de los cuales puedan ser sacrificados) y la sujeción de los poderes públicos a la ley" . Otros tribunales nacionales se han referido también a los límites de la democracia en relación con la protección de derechos fundamentales.*

Además, se deben considerar las cuatro sentencias condenatorias al Estado mexicano (2009-2010)[7]. Las cuales se refieren expresamente a que el ejercicio del control de

[7] Caso Rosendo Radilla Pacheco vs. Estados Unidos Mexicanos, excepciones preliminares, fon- do, reparaciones y costas, sentencia del 23 de noviembre de 2009, serie C, núm. 209, párr. 339; caso Fernández Ortega y otros vs. México, excepción preliminar, fondo, reparaciones y costas, sentencia del 30 de agosto de 2010, serie C, núm. 215, párr. 234; caso Rosendo Cantú y otra vs. México, excepción preliminar, fondo, reparaciones y costas, sentencia del 31 de agosto de 2010, serie C, núm. 216, párr. 219; y caso Cabrera García y Montiel Flores vs. México, excepciones preliminares, fondo, reparaciones y costas, sentencia del 26 de noviembre de 2010, párr. 225. en este último asunto se precisa que dicha obligación recae no sólo en los

convencionalidad es un deber por parte de los jueces y órganos vinculados a la administración de justicia, en todos los niveles para ejercerlo. Asimismo, es relevante la aceptación expresa de este tipo de control, que se desprende de la interpretación hecha por la Suprema Corte de Justicia de la Nación. Cuyo criterio más relevante es el siguiente:

> ***CONTROL DE CONVENCIONALIDAD EX OFFICIO EN UN MODELO DE CONTROL DIFUSO DE CONSTITUCIONALIDAD[8].*** *De conformidad con lo previsto en el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos,* ***todas las autoridades del país, dentro del ámbito de sus competencias, se encuentran obligadas a velar no sólo por los derechos humanos contenidos en la Constitución Federal, sino también por aquellos contenidos en los instrumentos internacionales celebrados por el Estado Mexicano, adoptando la interpretación más favorable al derecho humano de que se trate, lo que se conoce en la doctrina como principio pro persona.*** *Estos mandatos contenidos en el artículo 1o. constitucional, reformado mediante Decreto publicado en el Diario Oficial de la Federación de 10 de junio de 2011, deben interpretarse junto con lo establecido por el diverso 133 para determinar el marco dentro del que debe realizarse el control de convencionalidad ex officio en materia de derechos humanos a cargo del Poder Judicial, el que deberá adecuarse al modelo de control de constitucionalidad existente en nuestro país. Es en la función jurisdiccional, como está indicado en la última parte del artículo 133 en relación con el artículo 1o. constitucionales, en donde los jueces están obligados a preferir los derechos humanos contenidos en la Constitución y en los tratados internacionales, aun a pesar de las disposiciones en contrario que se encuentren en cualquier norma inferior. Si bien los jueces no pueden hacer una declaración general sobre la invalidez o expulsar del orden jurídico las normas que consideren contrarias a los derechos humanos contenidos en la Constitución y en los tratados (como sí sucede en las vías de control directas establecidas expresamente en los artículos 103, 105 y 107 de la Constitución), sí están obligados a dejar de aplicar las normas inferiores dando preferencia a las contenidas en la Constitución y en los tratados en la materia.*

---

"jueces", sino en general en todos los "órganos vinculados a la administración de justicia" de "todos los niveles" (sean locales o federales).

[8] Registro No. 160589 Localización: Décima Época Instancia: Pleno Fuente: Semanario Judicial de la Federación y su Gaceta Libro III, Diciembre de 2011 Página: 535 Tesis: P. LXVII/2011(9a.) Tesis Aislada Materia(s): Constitucional

Ahora bien, sin pretensión de ahondar en todos los supuestos, se señalarán algunas características y consecuencias que se desprenden del criterio hermenéutico contenido en el artículo 1o. constitucional y en las disposiciones antes citadas[9]:

1. **Los Destinatarios:** Todas las autoridades del estado mexicano, dentro de sus competencias, tienen que seguir este criterio interpretativo:
    i. Jueces: deben acudir a esta técnica de interpretación en todo caso relacionado con normas de derechos humanos en los asuntos de su competencia;
    ii. Legisladores: tendrán que adecuar la normativa existente utilizando este criterio y aplicarlo al emitir la norma;
    iii. Todos los órganos de la administración pública deberán ajustar su actuación conforme a la nueva pauta interpretativa de derechos humanos, especialmente cuando se trate de restricción de los mismos.
2. **Es un mandato constitucional "no disponible" por el intérprete.** Y para cumplirlo se tiene que:
    a. Crear una práctica sistemática y constante de dicha pauta interpretativa en todos los niveles.
    b. No puede nunca ser "optativo" o "facultativo" para el intérprete de la norma en materia de derechos humanos.
3. **Este criterio interpretativo se aplica con independencia del rango o jerarquía que tenga la norma en cuestión**, de tal manera que las normas que los contengan deberán interpretarse de conformidad con los derechos humanos previstos en la Constitución y en los tratados internacionales;
    a. todos los derechos humanos, sea cual sea su ubicación en el texto fundamental (como sucede con los derechos humanos de tipo laboral previstos en el artículo 123, por ejemplo);
    b. También a aquellos derechos humanos previstos en cualquier tratado internacional, sea cual sea su denominación o la materia que regule.
    c. También normas de carácter "adjetivas" relativas a derechos humanos.
    d. La expresión tratados internacionales debe comprender también la interpretación que establezcan los órganos que el propio tratado autoriza para su interpretación.
        i. Con mayor intensidad si existen órganos jurisdiccionales cuya misión es la aplicación e interpretación del tratado. Ejemplo:

[9]Ferrer Mac Gregor, *Eduardo, Interpretación conforme y control difuso de convencionalidad. El nuevo paradigma para el juez mexicano*. Instituto de Investigaciones Jurídicas UNAM, México.

1. Corte IDH, que "tiene competencia para conocer de cualquier caso relativo a la interpretación y aplicación de las disposiciones" del Pacto de san José.

Asimismo, derivado del expediente varios 912/2014, la Suprema Corte de Justicia de la Nación especificó que este tipo de control constitucional por parte de los jueces presupone realizar tres pasos interpretativos:

**A) Interpretación conforme en sentido amplio.** Ello significa que los jueces del país, al igual que todas las demás autoridades del Estado mexicano, deben interpretar el orden jurídico a la luz y conforme a los derechos humanos establecidos en la Constitución y en los tratados internacionales en los cuales el Estado mexicano sea parte, favoreciendo en todo tiempo a las personas la protección más amplia.

**B) Interpretación conforme en sentido estricto.** Ello significa que cuando hay varias interpretaciones jurídicamente válidas, los jueces deben, partiendo de la presunción de constitucionalidad de las leyes, preferir aquélla que hace a la ley acorde a los derechos humanos establecidos en la Constitución y en los tratados internacionales en los que el Estado mexicano sea parte, para evitar incidir o vulnerar el contenido esencial de estos derechos.

**C) Inaplicación de la ley cuando las alternativas anteriores no son posibles.** Ello no afecta o rompe con la lógica del principio de división de poderes y del federalismo, sino que fortalece el papel de los jueces al ser el último recurso para asegurar la primacía y aplicación efectiva de los derechos humanos establecidos en la Constitución y en los tratados internacionales de los cuales el Estado mexicano es parte.

De este modo, el marco interpretativo mencionado con anterioridad nos tiene que servir como referencia, ya que el Instituto no sólo tiene las facultades, sino también tiene la obligación de aplicarlo al momento de emitir cualquier regulación. Por lo mismo, los presentes lineamientos tienen que emitirse tomando en cuenta todas las facultades con las que cuenta el presente órgano constitucional autónomo.

### 1.2 Marco internacional en derechos humanos

#### 1.2.1. Criterios de la SCJN sobre la obligatoriedad de las fuentes jurídicas internacionales

De la misma manera que se estableció un marco nacional sobre derechos humanos que tiene que ser tomado en cuenta al momento del análisis, es importante que se tome en

consideración el marco internacional que, por criterios de la SCJN y en términos del artículo 1 constitucional, es ahora aplicable y vinculante en México. Así las cosas, primero se establecerán cuáles son los criterios que nos permiten hacer este análisis internacional y cuál es obligatoriedad jurídica de las convenciones y resoluciones aquí presentadas y, segundo, se establecerán los criterios que nos parecen más relevantes y que tuvieron que tomarse en cuenta para la creación de los lineamientos que nos competen.

El 15 de marzo de 2008, la Comisión Interamericana de Derechos Humanos sometió el caso de la presunta desaparición forzada de Rosendo Radilla Pacheco a la Corte IDH. La sentencia dictada fue condenatoria y se notificó al Estado Mexicano el 9 de febrero de 2010. El 26 de mayo, el entonces presidente de la SCJN formuló una consulta al Pleno de la SCJN para determinar la participación del Poder Judicial de la Federación en el cumplimiento de la sentencia, por lo que se formó el expediente "Varios 489/2010"[10].

En dicha sentencia, es destacable el Considerando Quinto, que declara la obligatoriedad de la aplicación de las sentencias de la Corte IDH para todos los órganos jurisdiccionales. Dicho considerando establece lo siguiente:

> *"**19.** Así, las resoluciones pronunciadas por aquella instancia internacional cuya jurisdicción ha sido aceptada por el Estado Mexicano, <u>son obligatorias para todos los órganos del mismo en sus respectivas competencias</u>, al haber figurado como Estado parte en un litigio concreto. Por tanto, para el Poder Judicial son vinculantes no solamente los puntos de resolución concretos de la sentencia, sino la totalidad de los criterios contenidos en la sentencia mediante la cual se resuelve ese litigio."*[11]

En el mismo considerando, la SCJN estableció la siguiente distinción respecto a la aplicación de las sentencias de la Corte IDH cuando el Estado Mexicano no sea parte del caso:

> *"20. Por otro lado, el resto de la jurisprudencia de la Corte Interamericana que deriva de las sentencias en donde el Estado Mexicano no figura como parte, tendrá el carácter de criterio orientador de todas las decisiones de los Jueces mexicanos, pero siempre en aquello que le sea más favorecedor a la persona, de conformidad con el artículo 1o. constitucional, cuya reforma se publicó en el*

---

[10] SCJN. *VARIOS 912/2012. "Caso Rosendo Radilla Pacheco"*. Seguimiento de Asuntos Resueltos por el Pleno de la Suprema Corte de Justicia de la Nación. Disponible en línea en: http://www2.scjn.gob.mx/AsuntosRelevantes/pagina/SeguimientoAsuntosRelevantesPub.aspx?ID=121589&SeguimientoID=225

[11] Pleno de la SCJN. *Varios 912/2012. Ejecutoria.* Semanario Judicial de la Federación y su Gaceta, Libro I, Octubre de 2011, Tomo 1, página 313.

*Diario Oficial de la Federación el diez de junio de dos mil once, en particular en su párrafo segundo, donde establece que: "Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia."*[12]

Esta determinación de la Suprema Corte implicó un cambio drástico en la impartición de justicia en México. A raiz de la misma comenzaron a surgir interrogantes acerca de la aplicación que las resoluciones internacionales podían tener dentro del sistema jurídico mexicano con base en lo establecido por el artículo 133 de la Constitución:

*"**Artículo 133.** Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados."*[13]

En la contradicción de tesis 293/2011, la Suprema Corte de Justicia de la Nación discutió la posición jerárquica que ocupan los tratados internacionales en materia de Derechos Humanos dentro del sistema jurídico mexicano y, con mayor especificidad, frente a la Constitución. El dilema jurídico planteado consistía en ubicar los Tratados Internacionales jerárquicamente debajo de la Constitución, pero encima de las leyes secundarias, o al mismo nivel de la Constitución. En la misma contradicción se planteó también el problema jurídico de determinar si la aplicación de la jurisprudencia emitida por la Corte Interamericana de Derechos Humanos era orientadora u obligatoria para los órganos jurisdiccionales.

Respecto del primer problema jurídico planteado, la Suprema Corte planteó lo siguiente:

*"De la interpretación literal, sistemática y originalista del contenido de las reformas constitucionales de seis y diez de junio de dos mil once, se desprende que las normas de derechos humanos, independientemente de su fuente, no se relacionan en términos jerárquicos, entendiendo que, derivado de la parte final del primer párrafo del citado artículo 1o., cuando en la Constitución haya una restricción expresa al ejercicio de los derechos humanos, se deberá estar a lo que indica la norma constitucional, ya que el principio que le brinda*

[12] Ibíd.

[13] México. *Constitución Política de los Estados Unidos Mexicanos*. México: 2015.

*supremacía comporta el encumbramiento de la Constitución como norma fundamental del orden jurídico mexicano, lo que a su vez implica que el resto de las normas jurídicas deben ser acordes con la misma, tanto en un sentido formal como material. [...]En este sentido, los derechos humanos, en su conjunto, constituyen el parámetro de control de regularidad constitucional, conforme al cual debe analizarse la validez de las normas y actos que forman parte del orden jurídico mexicano."*[14]

Este criterio implica un cambio significativo respecto a lo que inicialmente había establecido la propia SCJN en la sentencia del expediente "Varios 912/2010", pues ahora el parámetro del control de regularidad constitucional recae en los Derechos Humanos; y, lo más importante, se estableció que, cuando en la Constitución exista una restricción expresa al ejercicio de los derechos humanos, se deberá estar a lo que indica la norma constitucional.

Por otra parte, respecto al valor de la jurisprudencia emitida por la Corte Interamericana de Derechos Humanos, la SCJN determinó lo siguiente:

*"Los criterios jurisprudenciales de la Corte Interamericana de Derechos Humanos, con independencia de que el Estado Mexicano haya sido parte en el litigio ante dicho tribunal, resultan vinculantes para los Jueces nacionales al constituir una extensión de la Convención Americana sobre Derechos Humanos, toda vez que en dichos criterios se determina el contenido de los derechos humanos establecidos en ese tratado. La fuerza vinculante de la jurisprudencia interamericana se desprende del propio mandato establecido en el artículo 1o. constitucional, pues el principio pro persona obliga a los Jueces nacionales a resolver cada caso atendiendo a la interpretación más favorable a la persona."*[15]

Con lo anterior, también se modificó el planteamiento inicial de la SCJN en la sentencia del expediente "Varios 912/2010", pues se declaró la aplicación vinculante de toda la jurisprudencia emitida por la Corte Interamericana de Derechos Humanos.

### 1.2.2. Convenciones Internacionales y Criterios de la Corte Interamericana de Derechos Humanos

[14] SCJN. *Contradicción de Tesis 293/2011*. Pleno de la SCJN, Décima Época, Registro 2006224. Gaceta del Semanario Judicial de la Federación, Jurisprudencia. Libro 5, Abril de 2014, Tomo I, Tesis P./J.20/2014, Página 202.

[15] SCJN. *Contradicción de Tesis 293/2011*. Pleno de la SCJN, Décima Época, Registro 2006224. Gaceta del Semanario Judicial de la Federación, Jurisprudencia. Libro 5, Abril de 2014, Tomo I, Tesis P./J.21/2014, Página 204.

Dado el análisis anterior es importante considerar, en primer lugar, diversas Convenciones y normas que son aplicables de manera directa o indirecta a los presentes lineamientos. Después, es necesario establecer cuáles han sido los criterios relevantes en la materia que ha emitido la Corte Interamericana de Derechos Humanos y que son vinculantes según nuestro ordenamiento jurídico.

En cuanto a las Convenciones y Tratados Internaciones en materia de derechos humanos, el artículo 11 de la Convención Americana de Derechos Humanos (en adelante, la "CADH") protege al individuo frente a la posible interferencia arbitraria o abusiva del Estado, en los siguientes términos:

> *"11.2: Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación*
>
> *11.3: Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".*

De la misma manera, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos establece como un derecho fundamental la vida privada:

> *"1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
>
> *"2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."*

De la misma manera, se establece en el artículo 12 de la Declaración Universal de Derechos Humanos:

> *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."*

Y, por último, en el artículo 16 de la Convención sobre los Derechos del Niño:

*"1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación.*

*2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".*

Estos artículos tienen relevancia, ya que se centran en definir que la vida privada es un derecho reconocido internacionalmente. Éste, como se menciona en los artículos, no puede ser vulnerado arbitrariamente. Es decir, tiene que existir un criterio de protección que establezca en qué momento es válido intervenir en la vida privada y en qué momento no. Esto, es algo que tiene que determinarse claramente en los lineamientos.

En cuanto a los criterios relevantes de la Corte Interamericana de Derechos Humanos, como mencionamos anteriormente, para hablar de la existencia de un marco completo de derechos humanos es necesario analizar todos los supuestos vinculantes. Por lo mismo, no sólo es necesario estudiar los artículos de las convenciones, sino los criterios y límites que han sido establecidos por la Corte Interamericana de Derechos Humanos y que nos darán un criterio orientador sobre cuáles son los alcances y límites que se han establecido sobre los derechos anteriormente mencionados. Los casos para saber el alcance de la protección de derechos humanos que se analizan en este apartado son los siguientes:

- Caso Tristán Donoso Vs. Panamá
- Caso Fontevecchia y D'Amico Vs. Argentina.
- Caso Escher y otros Vs. Brasil.
- Asimismo, si bien no es un caso, debe considerarse el Reporte sobre la Libertad de Expresión de Frank la Rue.

Ahora bien, lo más relevante de este tema recae en que la protección de las comunicaciones privadas se ha ido ampliando, de modo que no sólo son objeto de salvaguarda el contenido de ellas, sino también aquellos datos que identifiquen la misma o que se encuentren relacionados con ella.

En este sentido, la Corte Interamericana de Derechos Humanos (en adelante, la "CIDH") ha interpretado el artículo 11 de la CADH en los casos *Tristán Donoso Vs. Panamá* y *Fontevecchia y D'Amico Vs. Argentina*. En estas sentencias, la CIDH llega a la conclusión de que la geolocalización, así como la simple retención de datos de las llamadas sin

considerar su contenido son propiamente una intervención de comunicaciones, y por lo tanto quedan incluidos dentro del ámbito de protección de la vida privada de la persona[16].

Al respecto, en el párrafo 55, del caso *Tristán Donoso Vs. Panamá*, la CIDH refirió textualmente:

> *"55. El artículo 11 de la Convención prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, enunciando diversos ámbitos de la misma como la vida privada de sus familias, sus domicilios o sus correspondencias. La Corte ha sostenido que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. Aunque las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención, se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección del derecho a la vida privada".*

Posteriormente, este mismo razonamiento fue reafirmado en los casos *Escher y otros Vs. Brasil* y *Fontevecchia y D'Amico Vs. Argentina*, en especial en los párrafos 113-114 y 49, respectivamente.

También, a pesar de no ser vinculante, resulta orientador el criterio del Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, que también hace alusión a algunos de los principios antes enlistados. Al efecto, éste señala:

> *"31. El Relator Especial [...] <u>Instó a los gobiernos a que explicaran detalladamente cómo sus políticas de vigilancia se ajustaban a los principios de proporcionalidad y necesidad</u>, de conformidad con las normas internacionales de derechos humanos y qué medidas habían tomado para prevenir abusos".* [17]

Asimismo, Frank la Rue señala que el uso de un concepto impreciso de seguridad nacional puede socavar los principios de la transparencia y rendición de cuentas:

---

[16] CIDH. *Caso Tristán Donoso Vs. Panamá. Excepción Preliminar, Fondo, Reparaciones y Costas*. Sentencia de 27 de enero de 2009. Serie C No. 193, párr. 55. CIDH. *Caso Fontevecchia y D'Amico Vs. Argentina. Fondo, Reparaciones y Costas*. Sentencia de 29 de noviembre de 2011. Serie C No. 237, párr. 49. CIDH. *Caso Escher y otros Vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas*. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 113 y 114.

[17] Asamblea General de Naciones Unidas. *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, 2013. Pág. 10.

*"60. El uso de un concepto impreciso de seguridad nacional para justificar limitaciones invasivas del goce de los derechos humanos plantea serias preocupaciones. Este concepto tiene una definición amplia y, por consiguiente, es vulnerable a la manipulación del Estado como medio de justificar medidas dirigidas a grupos vulnerables como defensores de los derechos humanos, periodistas o activistas. También permite justificar el secreto a menudo innecesario en torno a investigaciones o actividades de las fuerzas del orden, socavando los principios de la transparencia y la rendición de cuentas"*[18].

### 1.2.3. Derecho comparado

Si bien los criterios que se transcriben a continuación no tienen fuerza vinculante dentro del ordenamiento jurídico mexicano –como sí la tienen las fuentes jurídicas señaladas anteriormente-, es importante que se tomen en cuenta cómo buenas prácticas internacionales a las que es relevante acceder. Al efecto, primero, se establecerán algunos criterios relevantes de la Corte Europea de Derechos Humanos y el Tribunal de Justicia de la Unión Europea y, después, otras referencias que han sido relevantes en algunos de los casos más importantes que tenemos que considerar.

La Corte Europea de Derechos Humanos y el Tribunal de Justicia de la Unión Europea han establecido precedentes relevantes en materia de intervención de comunicaciones. El primero de ellos es la declaración de invalidez de la Directiva sobre la conservación de datos. Entre otros, es pertinente rescatar los siguientes argumentos vertidos en dicha declaración[19]:

1. Se señala que los datos que se conservan permiten saber con qué persona y de qué modo se ha comunicado con un abonado o un usuario registrado, determinar el momento y el lugar en la que se ha producido y conocer la frecuencia de las comunicaciones del abonado o del usuario con determinadas personas durante un periodo concreto.
2. Se estipula que, al imponer la conservación de estos datos y al permitir el acceso a las autoridades nacionales competentes, la Directiva se inmiscuye de manera especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal.

En consonancia con los anteriores criterios, y los que sostiene la CIDH respecto a la vulneración del derecho a la privacidad de las personas, existen diversos precedentes del

[18] Ibíd. Pág. 17.

[19] 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.

Tribunal Europeo de Derechos Humanos con criterios similares a los arriba citados. Estos precedentes son:

- Caso Klass y otros Vs. Alemania.
- Caso Halford Vs. Reino Unido.
- Caso Amann Vs. Suiza.
- Caso Copland Vs. Reino Unido.

Un criterio relevante sostenido por el Tribunal Europeo de Derechos Humanos versa sobre el principio de notificación. Al respecto, este Tribunal estableció que, una vez que cesa la vigilancia y transcurre el tiempo estrictamente necesario para que el propósito legítimo de la vigilancia no sea puesto en riesgo, se debe notificar al afectado:

> *"90. Por último, la Corte observa que en la legislación búlgara las personas sometidas a vigilancia secreta no son notificadas de este hecho en cualquier momento y en cualquier circunstancia. De acuerdo con la jurisprudencia del Tribunal de Justicia, el hecho de que las personas afectadas por tales medidas no sean informados de ello, mientras la vigilancia está en curso o incluso después de que haya cesado no puede por sí solo justificar la conclusión de que la interferencia no estaba justificada en los términos del párrafo 2 del artículo 8, ya que es el desconocimiento de la vigilancia lo que garantiza su eficacia. Sin embargo, tan pronto como la notificación se puede hacer sin poner en peligro el objetivo de la vigilancia después de su terminación, se deberá proporcionar información a las personas interesadas (véase Klass y otros, p 27, § 58;.. Mutatis mutandis, Leander, p 27, § 66; y, más recientemente, Weber y Saravia, § 135)"*[20].

### 1.2.4. Otros ejemplos internacionales relevantes a considerar

Por último, como parte de este apartado primero, se expondrán algunos ejemplos internacionales a considerar en: i) el registro y almacenamiento de datos, ii) el envío de los datos (plataforma y modo de envío); y iii) finalmente, algunas buenas prácticas desde la perspectiva de la sociedad civil.

**En el registro y almacenamiento de datos**

[20] 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.

Hoy en día en diversos países, se han definido los lineamientos que determinan el trato que deben tener los datos registrados que permiten identificar las comunicaciones de los usuarios. Estos lineamientos tienen como objetivo principal garantizar que en ningún momento se violen los derechos humanos de los usuarios. Es por ello que los lineamientos han sido elaborados con el propósito de garantizar la confidencialidad, seguridad y trato de toda la información resguardada derivada de una comunicación. Algunos ejemplos internacionales son los siguientes:

- *Directive 2006/24/EC of the European Parliament and of the Council. On the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Unión Europea).*
- *Regulation (EC) No 45/2001 of the European Parliament and of the Council. On the protection of individuals with regard to the processing of personal data by the community institutions and bodies and on the free movement of such data (Unión Europea).*
- *Regulation of Investigatory Powers Act 2000 (UK).*
- *Electronic Communicactions – The Data Retention 2014 (UK).*
- *Data Retention and Investigatory Powers Act 2014 (UK).*
- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigactions (EUA).*

En estos documentos se presentan todos los procesos que se deben seguir y respetar para evitar el trato indebido e inadecuado de los datos resguardados. Los lineamientos abarcan todo el universo de regulación requerida para dicho propósito, desde la identificación de las autoridades facultadas para pedir la información, los mecanismos de requisición, la autenticación, los medios de transferencia, hasta la definición de los procesos específicos a seguir para el resguardo y eliminación de los datos dentro de las redes de los proveedores de servicios de comunicaciones.

**En el envío de los datos (plataforma y modo de envío)**

La transferencia de los datos de comunicaciones, de geolocalización y de intervención entre los proveedores de servicios de comunicaciones y las autoridades, debe ser a través de interfaces electrónicas que garanticen la integridad y seguridad de la información, así

como la administración y gestión efectiva del tráfico entre ambas partes. Para ello el Instituto Europeo de Estandarización en Telecomunicaciones (ETSI) ha creado dos estándares fundamentales: *ETSI 102 656 y ETSI 102 657*. Estos estándares definen las características generales e indispensables que toda interfaz electrónica debe tener para la transferencia de datos críticos y sensibles, como lo son los transferidos entre las autoridades y los proveedores de servicios de comunicaciones.

Estos estándares internacionales permiten normalizar el proceso técnico de solicitud y de entrega de datos que soliciten las autoridades a los proveedores, de acuerdo a las leyes aplicables de cada país.

**Buenas prácticas desde la perspectiva de la sociedad civil**

Aunado a lo anterior, diversas organizaciones de la sociedad civil, como Artículo 19, Consumers International y Privacy International, crearon un documento titulado "*Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*". Dichos principios establecen un marco mínimo que, si bien no es vinculante, permite dilucidar las principales preocupaciones y guías que deben seguirse en la creación de normas relacionadas con la vigilancia de las comunicaciones, a efecto de respetar y salvaguardar los derechos humanos. De su análisis integral se desprende que la principal dirección de estos principios apunta hacia la necesidad de la previsión legal de un procedimiento que permita garantizar –entre otras- la privacidad de la persona, así como la creación de mecanismos que permitan transparentar el uso debido de la información. A continuación, se enlistan los principios previstos por este documento, así como una breve descripción de su contenido[21]:

| Tabla 2. Principios | |
|---|---|
| **Principio** | Contenido |
| **Legalidad** | La necesidad de prescripción legal de la limitación a los derechos humanos, así como su revisión periódica por medio de procesos legislativos o reglamentarios participativos. |
| **Objetivo legítimo** | Las leyes sólo deben permitir la Vigilancia de las Comunicaciones para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante, importante y necesario en una sociedad democrática. |
| **Necesidad** | Las leyes, acciones y autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar el objetivo legítimo planteado. |

[21] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. 2013. Disponible en: https://es.necessaryandproportionate.org/text

| | |
|---|---|
| **Idoneidad** | La vigilancia autorizada legalmente debe ser apropiada para cumplir el objetivo legítimo planteado. |
| **Proporcionalidad** | En todo momento debe considerarse que la vigilancia de comunicaciones es un acto altamente intrusivo que amenaza los cimientos de una sociedad democrática, por lo cual, las decisiones respectivas deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses. El Estado debe demostrar *ex ante* a una autoridad judicial:<br>1. Existencia de un alto grado de probabilidad de que un delito u amenaza específica para un fin legítimo ha sido o será llevado a cabo.<br>2. Existencia de un alto grado de probabilidad de que las evidencias de un delito grave o amenaza específica se conseguirán mediante el acceso solicitado a la Información Protegida.<br>3. Agotamiento previo o inutilidad de otras técnicas de investigación menos invasivas.<br>4. Que la información a la que se accederá estará limitada a lo relevante y material para el crimen o amenaza específica al fin legítimo alegado.<br>5. Que la información excedente no será retenida, sino destruida o devuelta con prontitud.<br>6. Sólo la autoridad específica tendrá acceso a la información y ésta será usada solo para los propósitos y durante el lapso temporal autorizados.<br>7. Que las actividades de vigilancia no menoscaban la esencia del derecho a la privacidad o libertades fundamentales. |
| **Autoridad Judicial Competente** | Las decisiones relacionadas con la vigilancia de comunicaciones deben ser realizadas por autoridad judicial competente –imparcial e independiente-. |
| **Debido Proceso** | Se exige de los Estados que aseguren que los procedimientos legales que rigen cualquier interferencia estén enumerados apropiadamente en la ley, practicados consistentemente y disponibles para el público general. |
| **Notificación del usuario** | A los sujetos a quienes se vigilen las comunicaciones debe notificársele de la decisión con tiempo e información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. La |

| | |
|---|---|
| | obligación de notificar es del Estado, pero los proveedores de servicios de comunicaciones deben tener la libertad de notificar a las personas de la vigilancia de comunicaciones, de forma voluntaria o bajo petición. |
| **Transparencia** | Los Estados deben ser transparentes sobre el uso y alcance de las leyes de vigilancia de comunicaciones; deben proporcionar a las personas información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de dichas leyes; no deben interferir con los proveedores de servicios en sus esfuerzos para publicar los procedimientos aplicados en la evaluación y cumplimiento de solicitudes de los Estados para la vigilancia. |
| **Supervisión pública** | Los estados deben establecer mecanismos independientes de supervisión para garantizar la transparencia y rendición de cuentas de la Vigilancia de las Comunicaciones. |
| **Integridad de las comunicaciones y sistemas** | Los estados no deben obligar a los proveedores de servicios o de "hardware" o "software" a desarrollar capacidad de vigilancia o de control de sistemas, ni a recoger o retener determinada información exclusivamente para fines de vigilancia de comunicaciones del Estado. No debe ser exigida la retención o recopilación de datos a priori. Las personas tienen derecho a expresarse anónimamente, por lo que los Estados deben abstenerse de obligar a identificar a los usuarios. |
| **Garantías para la Cooperación Internacional** | Los tratados de asistencia judicial recíproca y otros acuerdos celebrados por los Estados deben garantizar que cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte la estándar disponible con mayor nivel de protección para las personas. El principio de doble incriminación debe ser aplicado en el momento en que los Estados procuren asistencia para efectos de hacer cumplir su legislación interna. |
| **Garantías contra el acceso ilegítimo y derecho a recurso efectivo** | Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas y medios de reparación a las personas afectadas. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba derivada de dicha información. Se debe establecer en las leyes que el |

| | |
|---|---|
| | material resultante de vigilancia de comunicaciones no debe ser retenido, en su lugar, debe ser destruido o devuelto a los afectados. |

## 2. Análisis del Proyecto de Lineamientos

Tomando en consideración un análisis exhaustivo de los Lineamientos y lo vasto del marco de derechos humanos, tanto nacional como internacional, anteriormente mencionado, considero que, en el presente asunto, existen 11 problemas a los cuales el presente Proyecto no da solución, lo cual se traduce en la falta de mecanismos eficaces y respetuosos de los derechos humanos en los Lineamientos. A continuación se exponen dichos problemas:

**Problema 1. El art. 190 de la LFTR manda a establecer lineamientos a efecto de que la colaboración sea "efectiva" y "oportuna". Sin embargo, los presentes Lineamientos no logran dicha finalidad y tampoco veo un sistema robusto y seguro que garantice la salvaguarda de los datos personales, como lo promete el primer Lineamiento.**

Éste problema abarca la generalidad de los lineamientos respecto al sistema de colaboración entre autoridades y concesionarios. El sistema establecido, como se mencionó en la introducción, tiene varias deficiencias, entre ellas se encuentra la generación de una multiplicidad de opciones y plataformas para la solicitud, envío y recepción de los datos que no permiten que el sistema sea eficaz y que, al mismo tiempo, se resguarden debidamente los derechos humanos. Para este punto es importante observar el diagrama del anexo 1.

**Problema 2. No se establece la obligación de las autoridades de acreditar que cuentan con autorización judicial para efectuar ciertos requerimientos a los concesionarios y autorizados, como lo son los requerimientos relativos al acceso al registro de datos conservados, y lo deja a la interpretación de los Concesionarios.**

Al efecto, se considera que para ciertos requerimientos de información que realizan las autoridades a los concesionarios es necesario que exista una intervención judicial de por medio que los autorice. Para analizar lo anterior, conviene indicar que existen 3 tipos de requerimientos de información a efectuar a los concesionarios. Estos tipos de requerimientos están reconocidos en el art. 190 de la LFTR, que estipula:

> ***Artículo 190.*** *Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán: [...] IV. Contar con un área responsable disponible las veinticuatro horas del día y los trescientos sesenta y cinco días del año, para*

*atender **los requerimientos de información, localización geográfica e intervención de comunicaciones privadas** a que se refiere este Título.*

Como se puede observar, el primero consiste en requerir el acceso al registro de información o datos referido en el artículo 190, fracción I, de la LFTR, es decir en solicitar parte o toda la información histórica de una cierta línea, dicha información no abarca el contenido de la comunicación, sino sólo los datos que la identifican (en lo sucesivo, el "Acceso al Registro de Datos"). El segundo consiste en requerir la ubicación/localización geográfica de un determinado equipo vinculado a un número telefónico (en adelante, la "Geolocalización"). El tercer tipo consiste en una solicitar intervención de comunicaciones privadas, es decir en requerir el contenido mismo de la comunicación que se efectúa a través de una línea (en adelante, "Intervención de Comunicaciones").

Hasta el momento, respecto al requerimiento de Intervención de Comunicaciones, no se ha puesto en duda el hecho de que sí es necesario contar con una previa autorización judicial para solicitarlo. En consecuencia, nos centraremos únicamente en los requerimientos de Geolocalización y Registro de Datos, en donde existe duda sobre si es necesaria o no dicha autorización judicial. Sin embargo, es necesario hacer referencia a la Intervención de Comunicaciones, pues su estudio es indispensable para dilucidar si el Registro de Datos requiere de previa autorización judicial.

Desde mi perspectiva, en los lineamientos se debería establecer que para el Acceso al Registro de Datos, sí se necesita autorización judicial, mientras que, para el requerimiento de Geolocalización, no se necesita ésta.

Al respecto, los artículos 189 y 190 de la LFTR establecen lo siguiente:

> ***Artículo 189 LFTR.*** *Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos **están obligados a atender todo mandamiento** por escrito, fundado y motivado de la autoridad competente **en los términos que establezcan las leyes**.*
>
> ***Artículo 190 LFTR.*** *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** [...]*
> ***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**.*

Como se puede ver, el artículo 189 indica que todo mandamiento (refiriéndose genéricamente a cualquier tipo de requerimiento que las autoridades efectúen a los concesionarios) deberá atenderse *"en los términos que establezcan las leyes"*. Por su parte, el artículo 190 señala que la obligación de los concesionarios de colaborar con las autoridades, en materia de Geolocalización, deberá realizarse igualmente *"en los términos que establezcan las leyes"*. Este artículo también refiere que el requerimiento de entrega de datos conservados se hará *"de conformidad con las leyes aplicables"*.

En consecuencia, la LFTR establece literalmente que, para analizar los términos bajo los cuales deben realizarse los requerimientos, es necesario acudir a las demás leyes aplicables y no sólo a lo estipulado en la LFTR. En este sentido, se debe acudir a otras leyes para dilucidar si ciertos requerimientos necesitan de una autorización judicial de por medio o no. Pero, ¿Cuáles son esas leyes?

En primer lugar, los artículos 21, 73 y 89 de la Constitución señalan lo siguiente:

> ***Artículo 21 constitucional.*** *[...] **La seguridad pública** es una función a cargo de la Federación, el Distrito Federal, los Estados y los Municipios, que comprende la prevención de los delitos; la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala.*
>
> ***Artículo 73 constitucional.*** *El Congreso tiene facultad: [...] **XXIII.** Para expedir leyes que establezcan las bases de coordinación entre la Federación, el Distrito Federal, los Estados y los Municipios, así como para establecer y organizar a las instituciones de **seguridad pública** en materia federal, de conformidad con lo establecido en el artículo 21 de esta Constitución. [...] **XXIX-M.** Para expedir leyes en materia de **seguridad nacional**, estableciendo los requisitos y límites a las investigaciones correspondientes.*
>
> ***Artículo 89 constitucional.*** *Las facultades y obligaciones del Presidente, son las siguientes: [...] VI. Preservar **la seguridad nacional**, en los términos de la ley respectiva, y disponer de la totalidad de la Fuerza Armada permanente o sea del Ejército, de la Armada y de la Fuerza Aérea para la seguridad interior y defensa exterior de la Federación.*

En este sentido, existen dos grandes rubros de leyes. Aquellas que versan sobre la seguridad pública, que comprende la prevención de los delitos, la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas;

y las que tratan sobre seguridad nacional, que abarcan toda afectación o amenaza al Estado o a uno de sus elementos esenciales[22].

Respecto a las leyes en materia de seguridad nacional primordialmente se tienen las siguientes:

- La Ley de Seguridad Nacional (en adelante, la "LSN") y
- La Ley Orgánica del Ejército y Fuerza Aérea Mexicanos (en lo sucesivo, la "LOEFAM")

En relación con las leyes de seguridad pública, conviene indicar que, existen dos parámetros a tomar en consideración. El primero de ellos consiste en el marco legal aplicable antes de la entrada en vigor del Código Nacional de Procedimientos Penales (en adelante, el "CNPP"). Este primer marco consiste en: la Ley Federal Contra la Delincuencia Organizada, la Ley de la Policía Federal, y el Código Federal de Procedimientos Penales, entre otros. El segundo marco consiste en el marco aplicable después de la entrada en vigor del CNPP.

Para dilucidar qué parámetro debemos tomar en consideración, es necesario remitirse al artículo Trigésimo Séptimo Transitorio de la LFTR, el cual señala:

> *"**Para efectos de las autoridades de procuración de justicia** referidas en la fracción I del artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, continuarán vigentes las disposiciones de la Ley Federal de Telecomunicaciones **en materia de localización geográfica en tiempo real hasta en tanto entre en vigor el Código Nacional de Procedimientos Penales**."*

[22] Al respecto puede verse el art. 5 de la Ley de Seguridad Nacional que señala: ***Artículo 5.-*** *Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional: I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional; II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano; III. Actos que impidan a las autoridades actuar contra la delincuencia organizada; IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos; V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada; VI. Actos en contra de la seguridad de la aviación; VII. Actos que atenten en contra del personal diplomático; VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva; IX. Actos ilícitos en contra de la navegación marítima; X. Todo acto de financiamiento de acciones y organizaciones terroristas; XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.*

De esta manera, se deduce que el marco legal que se debe analizar es aquel posterior a la entrada en vigor del CNPP, pues mientras no se encuentre en vigor el CNPP, será aplicable sólo lo establecido en la ya abrogada LFT y no lo señalado en la LFTR.

Bajo este entendido, las leyes que resultan relevantes son:

- El CNPP
- Las leyes reformadas con posterioridad al CNPP

Únicamente resulta relevante lo señalado por el CNPP, pues si bien, siguen existiendo códigos estatales de procedimiento en materia penal, no obstante, cuando entre en vigor el sistema penal acusatorio en dichas entidades federativas, les aplicará sólo el CNPP en materia de procedimiento penal.

Bajo este contexto, la pregunta a dilucidar es: ¿qué dicen estas leyes sobre la necesidad de una autorización judicial para efectuar un requerimiento? En este momento, la distinción sobre los tipos de requerimiento a efectuar se vuelve relevante, pues las leyes establecen exigencias distintas según el tipo de requerimiento.

De esta manera, en la siguiente Tabla 3 se realiza un análisis de los dos tipos de leyes (seguridad pública y seguridad nacional) en relación con los tres tipos de requerimientos (Geolocalización, Intervención de Comunicaciones y Registro de Datos), a efecto de indicar si dichos requerimientos (un total de 6 tipos) requiere de autorización judicial o no.

| Tabla 3 | | | |
|---|---|---|---|
| **Tipo de seguridad** | **Tipo de requerimiento** | **¿Se requiere autorización judicial?** | **Fundamento legal** |
| **Seguridad pública** | **1.** Geolocalización | **No** | -Artículos 251, fracción XI, en relación con el 303 del CNPP.[23] |
| | **2.** Intervención de comunicaciones | **Sí** | -Artículos 252, fracción III, y el 291 del CNPP. [24] |

[23]**Artículo 251 CNPP.-** Actuaciones en la investigación que no requieren autorización previa del Juez de Control. No requieren autorización del Juez de control los siguientes actos de investigación: [...] XI. Las demás en las que expresamente no se prevea control judicial. **Artículo 303 CNPP.-** Localización geográfica en tiempo real. Cuando exista denuncia o querella, y bajo su más estricta responsabilidad, el Procurador, o el servidor público en quien se delegue la facultad, solicitará a los concesionarios o permisionarios o comercializadoras del servicio de telecomunicaciones o comunicación vía satélite, la localización geográfica en tiempo real de los equipos de comunicación móvil asociados a una línea que se encuentren relacionados con los hechos que se investigan en términos de las disposiciones aplicables.

| | | | |
|---|---|---|---|
| | **3.** Acceso al Registro de Datos | **Sí** | -Artículos 252, fracción III, [25] y el 291, párrafo segundo,[26] del CNPP. |
| **Seguridad nacional** | **4.** Geolocalización | **No existe expresamente esta facultad** | -La LSN y la LOEFAM no contemplan expresamente la facultad de requerir a los concesionarios la Geolocalización de los equipos (aunque podría argumentarse que se encuentra implícita en el artículo 33 de la LSN).[27] |

[24] **Artículo 252 CNPP.-** Actos de investigación que requieren autorización previa del Juez de control. Con excepción de los actos de investigación previstos en el artículo anterior, requieren de autorización previa del Juez de control todos los actos de investigación que impliquen afectación a derechos establecidos en la Constitución, así como los siguientes: [...] III. La intervención de comunicaciones privadas y correspondencia.
**Artículo 291 CNPP.-** Intervención de las comunicaciones privadas. Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas el Titular de la Procuraduría General de la República o los servidores públicos facultados en términos de su ley orgánica, así como los Procuradores de las Entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma. [...] La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido [...] Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.

[25] Ídem.

[26] **Artículo 291 CNPP.-** Intervención de las comunicaciones privadas. [...] La intervención de comunicaciones privadas, abarca todo un sistema de comunicación, o programas que sean fruto de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos, que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo.

[27] **Artículo 33 LSN.-** En los casos de amenaza inminente a los que se refiere el artículo 5 de esta Ley, el Gobierno Mexicano podrá hacer uso de los recursos que legalmente se encuentren a su alcance, incluyendo la información anónima.

| | | | |
|---|---|---|---|
| | **5.** Intervención de comunicaciones | **Sí** | -Artículos 34 y 35 de la LSN.[28] |
| | **6.** Acceso al Registro de Datos | **Sí** | -Artículos 34 y 35 de la LSN.[29] |

De los 6 tipos diversos de requerimientos que se pueden efectuar, en 4 de ellos sí se requeriría autorización judicial, en 1 no se necesitaría y 1 caso sería ilegal el efectuarlo, pues las leyes en materia de seguridad nacional no contemplan su realización.

Lo anteriormente expuesto puede traducirse en que, conforme al marco de la LFTR y de las demás leyes en materia de seguridad pública y nacional, para que una autoridad realice un requerimiento de Acceso al Registro de Datos y de Intervención de Comunicación a un concesionario es necesario una autorización judicial. Mientras que, para que una autoridad realice un requerimiento de Geolocalización, no es necesaria dicha autorización.

Para acabar con la exposición de esta primera opción, conviene señalar que, del cuadro anterior, se aprecia que los fundamentos legales más discutibles pueden ser aquellos que sustentan que se necesita una autorización judicial en aquellos requerimientos relativos al Acceso al Registro de Datos (tipo de requerimientos 1 y 6). Al respecto, es necesario hacer las siguientes precisiones.

En primer lugar, el artículo 291 del CNPP, párrafo segundo, establece que:

> "**Art. 291 CNPP.** *Intervención de las comunicaciones privadas. [...] La intervención de comunicaciones privadas, abarca todo un sistema de comunicación, o programas que sean fruto de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así*

[28] **Artículo 34 LSN.-** De conformidad con lo dispuesto por el párrafo noveno del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro deberá solicitar en los términos y supuestos previstos por la presente Ley, autorización judicial para efectuar intervenciones de comunicaciones privadas en materia de Seguridad Nacional. Se entiende por intervención de comunicaciones la toma, escucha, monitoreo, grabación o registro, que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología. **Artículo 35 LSN.-** La solicitud a que se refiere el artículo anterior sólo procederá cuando se esté en uno de los supuestos que se contemplan en el artículo 5 de la presente Ley. En ningún otro caso podrá autorizarse al Centro la intervención de comunicaciones privadas. El Poder Judicial de la Federación, de acuerdo con su ley orgánica, determinará los juzgados que deban conocer de las solicitudes que en materia de Seguridad Nacional se presenten para intervenir comunicaciones privadas.

[29] Ídem. **Artículo 34 LSN.-** [...] Se entiende por intervención de comunicaciones la toma, escucha, monitoreo, grabación o registro, que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología.

*como archivos electrónicos, que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo."*

De ese modo, el CNPP protege no sólo el contenido de la comunicación, sino en general todo el *"sistema de comunicación"*, a tal grado que, también protege el registro/grabación/conservación de los *"datos que identifiquen la comunicación"*.

Por su parte, los artículos 34 y 35 de la LSN señalan que:

***Artículo 34 LSN.-*** *De conformidad con lo dispuesto por el párrafo noveno del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro deberá solicitar en los términos y supuestos previstos por la presente Ley, autorización judicial para efectuar intervenciones de comunicaciones privadas en materia de Seguridad Nacional. Se entiende por intervención de comunicaciones la toma, escucha, monitoreo,* ***grabación o registro, que hace una instancia autorizada,*** *de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología.*

***Artículo 35 LSN.-*** *La solicitud a que se refiere el artículo anterior sólo procederá cuando se esté en uno de los supuestos que se contemplan en el artículo 5 de la presente Ley. En ningún otro caso podrá autorizarse al Centro la intervención de comunicaciones privadas. El Poder Judicial de la Federación, de acuerdo con su ley orgánica, determinará los juzgados que deban conocer de las solicitudes que en materia de Seguridad Nacional se presenten para intervenir comunicaciones privadas.*

Ahora bien, la SCJN se ha pronunciado respecto a la necesidad de proteger las comunicaciones privadas, estableciendo ciertos límites y estándares que tienen que servir como guía al Instituto para la elaboración de los Lineamientos. Los criterios, son aquellos que se mencionaron y explicaron en el primer apartado del presente voto y que llevan por rubro: *"DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SUS DIFERENCIAS CON EL DERECHO A LA INTIMIDAD.*[30] *, DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE*

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

*IDENTIFICAN LA COMUNICACIÓN.*[31] *COMUNICACIONES PRIVADAS. EL DERECHO A SU INVIOLABILIDAD, CONSAGRADO EN EL ARTÍCULO 16, PÁRRAFO NOVENO, DE LA CONSTITUCIÓN FEDERAL, ES OPONIBLE TANTO A LAS AUTORIDADES COMO A LOS GOBERNADOS, QUIENES AL TRANSGREDIR ESTA PRERROGATIVA INCURREN EN LA COMISIÓN DE UN ILÍCITO CONSTITUCIONAL".*[32]

Aunado a lo anterior, como también se estableció en el primer apartado, en los casos *Tristán Donoso vs Panamá, Fontevecchia y D´amico vs Argetina, Escher y otros vs Brasil*, así como en el Reporte de Frank la Rue y en los Principios internacionales sobre vigilancia de las comunicaciones, se ha establecido que la protección de las comunicaciones abarca no sólo el contenido de éstas, sino aquellos datos que las identifiquen. Es decir, el objeto que se protege de una comunicación no sólo es el mensaje que se transmite, sino cualquier dato que pueda identificar el proceso comunicativo, realizado éste a través de cualquier medio o tecnología.

Ahora bien, los artículos 252, fracción III, y el 291, párrafo segundo, del CNPP y 34 y 35 de la LSN llevarían a las autoridades en materia de seguridad pública y nacional a requerir el Acceso al Registro de Datos al que se refiere el artículo 190 fracción II de la LFTR. Los datos contenidos en esta fracción son, en efecto, datos que permiten identificar el contenido de las comunicaciones, por ejemplo: el nombre y domicilio del suscriptor; número de destino; y la fecha, hora y duración de la comunicación, entre otros.

En consecuencia, si el CNPP y la LSN facultan a las autoridades a acceder al Registro de Datos señalado en el art. 190 de la LFTR, estos deben interpretarse a la luz del marco constitucional en materia de protección al derecho de privacidad e inviolabilidad de las comunicaciones privadas y atendiendo al principio *pro persona*. Lo anterior a efecto de considerar que los artículos 252, fracción III, y el 291, párrafo segundo, del CNPP, así como los artículos 34 y 35 de la LSN consideran que el Acceso al Registro de Datos (contemplado en los arts. 189 y 190 de la LFTR) por parte de las autoridades constituyen formalmente una Intervención de Comunicaciones y, por ende, requiere de previa autorización judicial.

---

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

[32] Época: Novena Época. Registro: 190652. Instancia: Segunda Sala. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XII, Diciembre de 2000 Materia(s): Constitucional. Tesis: 2a. CLX/2000. Página: 428. Amparo en revisión 2/2000. Norma Angélica Medrano Saavedra. 11 de octubre del año 2000. Unanimidad de cuatro votos. Ausente: José Vicente Aguinaco Alemán. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: María Elena Rosas López.

Incluso, el requerimiento de Acceso al Registro de Datos se encuentra protegido por lo dispuesto en el último párrafo del artículo 190 de la LFTR que señala:

> ***Art. 190 LFTR.*** *[...] Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.*

Por lo anteriormente expuesto, se considera que para el requerimiento de Acceso al Registro de Datos, sí se necesita autorización judicial.

**Problema 3. No existe un estándar claro, ni de los requisitos de cuándo los concesionarios y autorizados están obligados a atender un requerimiento de geolocalización. Asimismo no se pide a las autoridades que fundamenten y motiven estas solicitudes en los principios de necesidad, idoneidad y proporcionalidad.**

Ahora bien, en lo que respecta a la Geolocalización, ésta no necesita autorización judicial. Sin embargo, eso no significa que pueda ser aplicada en todos los casos y de manera indiscriminada. Al respecto, la SCJN ha propuesto el estándar a través de la Acción de Inconstitucionalidad 32/2012 –que ya fue referido anteriormente-. Sin embargo, dentro de los lineamientos no se observa ningún criterio ni estándar que permita ver que la geolocalización se utilizará de manera estricta y como una medida importante de excepción.

**Problema 4. Cada autoridad que pretenda usar el sistema o hacer requerimientos, debería tener la carga de la prueba de acreditar que tiene facultades legales expresas de geolocalizar o intervenir comunicaciones, incluyendo el acceso al registro de datos para tener acceso al uso del sistema. El proyecto sin embargo, no requiere de ello sino que son los Concesionarios y Autorizados quienes habrán de decidir si un requerimiento dado proviene de autoridad debidamente facultada o no. Eso es inaceptable.**

En la consulta pública hubo manifestaciones en las que se indicó que no había claridad en cuanto a quién es una autoridad facultada para efectuar un requerimiento. Esto se traduce no sólo en una preocupación por parte de los regulados, sino también de la sociedad civil, pues si no se establece con claridad quién puede realizar un requerimiento a los concesionarios podrían crearse incluso incentivos para que cualquier autoridad que se considere a sí misma como autoridad en materia de seguridad o procuración de justicia realice un requerimiento.

Si bien la preocupación principal puede traducirse en responder a la pregunta ¿Quién es propiamente una autoridad facultada? No obstante, la preocupación inmersa se encuentra en dilucidar ¿Quién debe establecer quién es una autoridad facultada?

Antes de entrar al análisis de este problema conviene dilucidar quiénes son, en términos generales, "las autoridades" que resultan relevantes para los presentes Lineamientos. El artículo 190, fracción I, señala tres tipos de autoridades: i) de seguridad, ii) de procuración de justicia y iii) de administración de justicia. Sin embargo, el mismo artículo 190 establece que los Lineamientos del Instituto versan sobre la colaboración de los concesionarios y autorizados con "las autoridades referidas en el artículo 189 de la LFTyR". De este modo para determinar las autoridades relevantes para los presentes Lineamientos debemos acudir a este artículo:

> ***Artículo 189 LFTyR.*** *Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado* ***de la autoridad competente en los términos que establezcan las leyes****.*
>
> ***Los titulares de las instancias de seguridad y procuración de justicia*** *designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.*

En consecuencia, en términos generales, las autoridades relevantes para los Lineamientos son las siguientes (en adelante, las "autoridades facultadas"):

i) Las autoridades competentes en los términos que establezcan las leyes (señaladas en el párrafo primero del art. 189)
ii) Las instancias de seguridad y procuración de justicia (señaladas en el párrafo segundo del art. 189 y que se circunscriben dentro del inciso "i" anterior)

Ahora bien, la solución a este problema que considero adecuada y que debe incluirse en los Lineamientos consiste en que el Instituto debía establecer un listado (dentro de los Lineamientos) de quiénes son las autoridades facultades.

En este sentido, conviene preguntarse si ¿el Instituto cuenta con las atribuciones suficientes para determinar quiénes son las autoridades facultades para efectuar los requerimientos a los concesionarios y autorizados? Para determinar esto conviene analizar a detalle las competencias que le otorga la LFTyR. Al respecto, ésta señala:

> ***Art. 190 LFTyR.*** *[...] **I.** [...] **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 [...]*
>
> ***II.*** *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.*
>
> ***Artículo 15 LFTyR.*** ***Para el ejercicio de sus atribuciones corresponde al Instituto:*** *XXIX.* ***Coordinarse con las autoridades*** *federales, del Gobierno del Distrito Federal, estatales y municipales, así como con los órganos autónomos,* ***a fin de recabar información y documentación necesaria para el ejercicio de sus atribuciones*** *[...]*

Del artículo 190 de la LFTyR se desprende que el Instituto tiene facultad para dictar los lineamientos que los concesionarios y autorizados deben adoptar para que la colaboración con las autoridades sea efectiva y oportuna. Bajo este entendido, la cuestión consiste en determinar si para lograr una colaboración autoridades-concesionarios efectiva y oportuna es necesario que el Instituto elabore una lista con las autoridades que están facultadas para efectuar los requerimientos.

No obstante, esta cuestión a determinar puede llegar a ser muy ambigua, pues en aras de una colaboración efectiva y oportuna, podrían ejercerse un amplio número de facultades. Por tal razón, en vez de entrar a un análisis a fondo sobre este punto, conviene resaltar dos obligaciones que tiene el Instituto a la luz de los artículos 15, fracción XXIX, y 190, fracciones I y II, de la LFTyR.

Al respecto, el Instituto tiene la obligación de: i) escuchar a las autoridades a que se refiere el artículo 189 para establecer los lineamientos, y ii) recibir, por parte de las autoridades referidas en el artículo 189, **los mecanismos** que éstas determinen para la solicitud y entrega en tiempo real de los datos. Dichas obligaciones deben concretarse antes de que el Instituto emita los Lineamientos.

Como ya se señaló anteriormente, las autoridades facultadas son, en términos generales, aquellas referidas en el artículo 189 de la LFTR. La pregunta es entonces, si el Instituto tiene que escuchar a las autoridades facultadas y recibir de ellas mismas los mecanismos para la entrega y solicitud de datos, ¿Acaso no debe antes, por lógica, determinar quién es

una autoridad facultada? Supóngase que una autoridad en materia legislativa, una autoridad aduanera o, incluso, un grupo de autodefensa acuden ante el Instituto a presentar sus mecanismos en el que consideran adecuado que se les entreguen los datos de los usuarios ¿el Instituto debe recibir y dar el cauce debido a estos mecanismos? También puede suponerse el supuesto contrario, es decir, en caso de que ninguna autoridad acuda por su propia iniciativa, forzosamente, el Instituto, con fundamento en los artículos 15 y 190 tendría que mandar a llamar a las autoridades facultadas para escucharlas, pero, al llamarlas ¿No estaría ya determinando quiénes son propiamente dichas autoridades?

De este modo ¿no es necesario, entonces, que el Instituto determine —desde antes de la emisión de los Lineamientos— quién es una autoridad facultada, a efecto de dar cumplimiento a estas dos obligaciones que le impone el artículo 190 de la LFTR? La respuesta es muy clara, si el Instituto no interpreta quién es un autoridad facultada prácticamente estaría incumpliendo con la LFTR.

En consecuencia, a partir de las obligaciones ya señaladas (que tiene que cumplir el Instituto antes de la emisión de los Lineamientos) resulta claro qué el Instituto sí tiene facultades para determinar quién es una autoridad facultada.

Ante esto, las autoridades podrían argumentar que el Instituto no puede restringir su ámbito competencial, ni interpretar las normas que rigen sus facultades y composición e, incluso, que no es ninguna autoridad en materia de seguridad pública y nacional. Sin embargo, como ya ha quedado expuesto, la LFTR refiere en diversas ocasiones que debe acudirse a lo que otras leyes dispongan. En el mismo artículo 189 –que contempla a las autoridades facultadas-, se define a estas autoridades como: *"la autoridad competente en los términos que establezcan las leyes."*

Por lo anteriormente expuesto, se considera que el Instituto debe establecer un listado (dentro de los Lineamientos) que señale quiénes son las autoridades facultades, de acuerdo a las facultades conferidas en las diversas leyes antes mencionadas en la tabla 1.

**Problema 5. Para que un requerimiento se atienda por los concesionarios o autorizados es necesario que alguien lo valide previamente. De otro modo, las autoridades no tendrían algún límite o freno para efectuar dichos requerimientos Pese a esto, el Proyecto no se pronuncia explícitamente sobre quién debe realizar esta validación e, implícitamente, lo deja al juicio de los concesionarios y autorizados. Esto ocasiona una privatización de la justicia en temas tan importantes como la materia penal.**

Existe una gran preocupación respecto a la validación de los requerimientos, pues el Proyecto de Lineamientos impone a los regulados la obligación de "validar" los

requerimientos. Sin embargo, los regulados no son autoridades públicas ni expertas en materia penal, ni tienen facultades para revisar la fundamentación y motivación de los requerimientos. Del mismo modo, a la sociedad civil le preocupa que sea un concesionario o autorizado (es decir, un particular) quien decida sobre la procedencia o no de un requerimiento.

En este punto se vuelve relevante la distinción planteada anteriormente en el Problema 1, en el cual se indica que hay tres tipos de requerimientos: i) el de Acceso al Registro de Datos, ii) el de Geolocalización y iii) el de Intervención de Comunicaciones. Ahora bien, el artículo 189 de la LFTR señala que: "*los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente* <u>*en los términos que establezcan las leyes*</u>".

Pero ¿Qué dicen las leyes (en materia de seguridad) al respecto? Como ya se indicó anteriormente, las leyes contemplan que, para el caso de Intervención de Comunicaciones (que incluye el requerimiento de Acceso al Registro de Datos) sí se necesita autorización judicial, mientras que, para el de Geolocalización no se necesita.

De este modo, en el caso de Intervención de Comunicaciones (que incluye el requerimiento de Acceso al Registro de Datos) el juez de control validaría los respectivos requerimientos. La ventaja de que sea un juez quien valide el requerimiento es que es una autoridad: i) formalmente ajena e independiente a la autoridad requirente, ii) especializada en el tema, iii) que podría realizar una validación del requerimiento conforme a los casos en concreto que se le presenten (es decir, el juez podrá conocer los méritos del caso y evaluar si dicho caso amerita o no efectuar un requerimiento, y no simplemente limitarse a hacer un *check list*); y iv) que la práctica internacional contempla la autorización de jueces para requerimientos de este tipo.

En contraste, en los casos de Geolocalización –que, como ya se señaló, no necesitan de previa autorización judicial- tendríamos que encontrar otra solución. Dicha solución consiste en que el Instituto cree una ventanilla única que valide los requerimientos. La finalidad de dicha ventanilla electrónica es que ésta centralice y valide los requerimientos efectuados a los concesionarios, en materia de Geolocalización.

Como ya se ha dicho, el fundamento para que el Instituto establezca una ventanilla de este tipo se encuentra en el art. 190, en relación con sus facultades para lograr una colaboración efectiva y oportuna entre autoridades-concesionarios.

**Problema 6. El formato y el contenido que habrán de incluir los requerimientos, son potestativos y no obligatorios, lo cual trae como consecuencia que las autoridades**

**pueden utilizar cualquier formato y dar la información que deseen, ocasionando incertidumbre, ineficacias o abusos. Asimismo hace falta incluir requisitos adicionales a los establecidos (ejemplo el nombramiento de la autoridad designada, como servidor público de la autoridad facultada).**

Los Lineamientos incluyen, como Anexo I, sólo un formato. Dicho formato podrá ser utilizado por las autoridades al momento de realizar un requerimiento a un concesionario o autorizado. Sin embargo, se observa que se ha propuesto el uso de más de un formato para atender las solicitudes.

Desde nuestra perspectiva, es necesario que se contemple más de un solo formato, es decir, que se contemple un formato para cada tipo de requerimiento. Como ya se ha expuesto anteriormente, existen 3 tipos de requerimientos de información a efectuar a los concesionarios, por lo que deberían existir un número igual de formatos.

Se considera que el tratar los 3 requerimientos bajo 3 diferentes formatos facilitaría la labor a los concesionarios y autorizados, pues para cada caso, ellos sabrían de una manera muy fácil qué se necesita: si es proporcionar la ubicación del dispositivo, el registro de datos o intervenir las comunicaciones. De este modo, los concesionarios podrían dar una atención más adecuada a cada requerimiento.

Del mismo modo, existe una preocupación en cuanto a los requisitos mínimos que deben contener los requerimientos a efectuar a los concesionarios.

Sin embargo, desde nuestra perspectiva, podrían exigirse mayores requisitos a las autoridades. Como se expuso en los primeros capítulos de este documento, en la intervención de comunicaciones privadas deben contemplarse, por lo menos, los siguientes principios: legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autoridad judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y sistemas, garantías para la cooperación internacional y garantías contra el acceso ilegítimo y derecho a recurso efectivo.

Bajo estos principios, se sugiere incluir los siguientes requisitos para cada tipo de requerimiento : 1) que se establezca la necesidad y el objetivo que motiva el requerimiento (esto con base en el principio de necesidad), 2) justificación de que es el único medio para alcanzar el objetivo mencionado con anterioridad o que es el menos propenso a vulnerar los derechos humanos (con base en el principio de idoneidad) y 3) que la medida es proporcional con el objetivo que se desea alcanzar (con base en el principio de proporcionalidad).

En consecuencia deberían agregarse los requisitos anteriormente señalados, en aras de proteger en mayor medida el derecho a la privacidad.

Por último, el uso de estos formatos y su llenado íntegro y completo deberían ser una obligación por parte de las autoridades requirentes y no simplemente algo potestativo.

**Problema 7. Respecto al principio y obligaciones en materia de transparencia, hace falta incluir en los Lineamientos dos elementos adicionales: i) la notificación al usuario cuya línea o dispositivo fue objeto de un requerimiento, con posterioridad a éste cuando ya no se ponga en riesgo la investigación misma y ii) que las autoridades facultades proporcionen información estadística sobre los requerimientos que llevaron a investigaciones exitosas.**

Los Lineamientos contienen un conjunto de obligaciones en materia de transparencia que buscan que la actuación de las autoridades y de los concesionarios en relación con los requerimientos sea pública en la medida de lo posible. Sin embargo, estas obligaciones son insuficientes considerando el estándar internacional y las mejores prácticas en la materia. En especial, hace falta establecer la obligación de notificar al usuario con posterioridad a la intervención, y que las autoridades proporcionen información sobre las investigaciones que han sido exitosas.

Por lo mismo, es necesario que se contemplen dos elementos adicionales en los Lineamientos: i) la notificación al usuario con posterioridad a la intervención y ii) que las autoridades proporcionen información sobre los requerimientos que llevaron a investigaciones que han sido exitosas.

En el marco estudiado, se aprecia que a nivel internacional existen diversas prácticas en materia de transparencia en la intervención de comunicaciones. Como muestra de esto, dos principios sobre la intervención de comunicaciones contenidos en los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* -que ya fueron referidos anteriormente en el apartado primero- señalan lo siguiente:

> ***Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (...) Notificación del Usuario:*** *Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados de la decisión de autorizar la Vigilancia de Comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación solo se justifica en las siguientes circunstancias:*

*1. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; y*
*2. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y*
*3. El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.*
*La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones deben tener la libertad de notificar a las personas de la Vigilancia de las Comunicaciones, de forma voluntaria o bajo petición.*

***Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (...) Transparencia:*** *Los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades. Deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos. Los Estados deben proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la Vigilancia de las Comunicaciones. Los Estados no deberían interferir con los proveedores de servicios en sus esfuerzos para publicar los procedimientos que aplican en la evaluación y el cumplimiento de solicitudes de los Estados para la Vigilancia de Comunicaciones, se adhieran a esos procedimientos, y publicar los registros de las solicitudes de los Estados para la Vigilancia de las Comunicaciones.*

Asimismo, en el Informe A/HRC/23/40 de 2013 de Frank la Rue, Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, se menciona lo siguiente:

*"VIII. Conclusions and recommendations [...] C. Increasing public access to information, understanding and awareness of threats to privacy*
*91. States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose.*

*92. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.*
*93. States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance of communications."*

Teniendo en consideración lo anteriormente citado, es necesario que los Lineamientos contemplen dos cuestiones relacionadas con la transparencia.

La primera cuestión a incluir consiste en es que el usuario debe ser notificado del requerimiento con posterioridad a su realización. Ahora bien, la segunda cuestión que debe incluirse en los Lineamientos consiste en establecer que las autoridades deben hacer pública la información sobre las investigaciones que han sido exitosas y en las que se han utilizado los requerimientos. Es decir, lo importante es saber si, a partir de la información obtenida por medio de un requerimiento, se logró una investigación o prevención exitosa. Esto permitiría a la sociedad evaluar si los requerimientos efectuados son en realidad un medio efectivo para lograr investigaciones exitosas o si están siendo usados de manera ineficaz.

**Problema 8. Hace falta establecer que el Instituto debe publicar, en coordinación con las autoridades, un listado de las autoridades designadas. Esto a efecto de que los concesionarios y autorizados tengan certidumbre respecto a qué autoridades pueden enviarles requerimientos.**

El Instituto podría simplificar la labor de los regulados y propiciar la coordinación efectiva al establecer un listado de las autoridades designadas, es decir de aquellas que han sido designadas por los titulares de las instancias de seguridad y procuración de justicia.

Por lo mismo, se considera indispensable que, a efecto de dar mayor certeza y facilitar la labor de los concesionarios de saber quién es una autoridad designada, el Instituto publique y actualice una lista de este tipo de autoridades.

Si bien el Diario Oficial de la Federación es público y cualquier persona –como los concesionarios y autorizados- pueden acceder a él y verificar quién es una autoridad designada, es necesario que, en términos del art. 190 de la LFTR el Instituto establezca Lineamientos que propicien una colaboración efectiva y oportuna. Para lograr dicha finalidad, se sugiere establecer este listado.

Esta lista no tendría ningún efecto de validez sobre las autoridades, pero sí un efecto de lograr una colaboración "efectiva" y "oportuna". Es decir, para que dichos acuerdos sean válidos, las autoridades necesitarían publicar su Acuerdo en el Diario Oficial de la Federación, como señala la LFTR, sin necesidad de que se encuentre en la lista del Instituto. Sin embargo, esta solución, aunada al listado de autoridades facultadas que se sugirió anteriormente que estableciera el Instituto, daría plena certeza a los concesionarios y autorizados, pues sabrían qué autoridad tiene facultades para efectuarles un requerimiento y, posteriormente, en específico el servidor público designado para efectuarlo.

Al efecto, el Instituto podría establecer una obligación de las autoridades de notificarles sus acuerdos de designación para que éste elabore y actualice un listado, o bien, podría obtenerlo directamente del Diario Oficial de la Federación.

**Problema 9. Es necesario establecer un conjunto de medidas sistematizadas para todas las partes involucradas en la colaboración, de protección de datos de los usuarios.**

Los Lineamientos no son claros en el tipo de obligaciones que tienen tanto los concesionarios y autorizados (dado que, en general todos los estándares se establecen como una potestad y no como una obligación) como las autoridades respecto a la protección de los datos de los usuarios.

El Instituto Federal de Acceso a la Información y Protección de Datos (ahora, el Instituto Nacional de Acceso a la Información y Protección de Datos, en adelante, el "INAI") dirigió una opinión al Proyecto de Lineamientos al Instituto. Dicha opinión fue dirigida con fundamento en lo siguiente:

> *"Por su parte, los artículos 40 de la Ley Federal de Protección de Datos Personales y 77 y 78 de su Reglamento establecen que el primer ordenamiento se constituye en el marco normativo que las dependencias deben observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda con la coadyuvancia del IFAI, ya sea petición de la dependencia de que se trate, o bien, cuando el Instituto advierta la necesidad de emitir o modificar regulación específica que involucre el tratamiento de datos personales."*

Este fundamento supone implícitamente que el Instituto cuenta con facultades para ejercer lo dispuesto por el artículo 40 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, la "LFPDPPP") y en los artículos 77 y 78 de su Reglamento:

> ***Artículo 40 LFPDPPP.-*** *La presente Ley constituirá el marco normativo que las dependencias deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del Instituto.*
>
> ***Artículo 77 Reglamento de la LFPDPPP.-*** *Emisión de regulación secundaria. Cuando la dependencia competente, atendiendo a las necesidades que advierta sobre el sector que regule, determine la necesidad de normar el tratamiento de datos personales en posesión de los particulares podrá, en el ámbito de sus competencias, emitir o modificar regulación específica, en coadyuvancia con el Instituto.*

Asimismo, cuando el Instituto, derivado del ejercicio de sus atribuciones, advierta la necesidad de emitir o modificar regulación específica para normar el tratamiento de datos personales en un sector o actividad determinada, podrá proponer a la dependencia competente la elaboración de un anteproyecto.

> ***Artículo 78 Reglamento de la LFPDPPP.-*** *Mecanismos de coordinación. Para la elaboración, emisión y publicación de la regulación a que se refiere el artículo 40 de la Ley, la dependencia y el Instituto establecerán los mecanismos de coordinación correspondientes.*

En todos los casos, la dependencia y el Instituto, en el ámbito de sus atribuciones, determinarán las disposiciones que normen el tratamiento de datos personales en el sector o actividad que corresponda.

En principio, estos artículos dotarían de competencia al Instituto para establecer regulación (en coordinación con el INAI) a efecto de proteger los datos personales en materia de servicios de telecomunicaciones. Sin embargo, el artículo 2 del Reglamento de la LFPDPPP parece acotar esta facultad a las "dependencias de la administración pública federal" –y no a órganos constitucionales autónomos- en los siguientes términos:

> ***Artículo 2 Reglamento de la LFPDPPP.-*** *Además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente Reglamento se entenderá por: I. Dependencias: Las señaladas en el artículo 26 de la Ley Orgánica de la Administración Pública Federal [...]*

Pese a esto, debe considerarse que el Reglamento no es del todo aplicable a al Instituto, como un órgano autónomo, pues el fundamento de un Reglamento es el artículo 89 constitucional y aplicable sólo para la Administración pública federal. También,

considérese que la misma LFTR señala que, respecto a la protección de datos personales, será aplicable lo dispuesto por la LFPDPPP:

> ***Artículo 190 LFTyR.*** *[...] II. [...] 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.*

Incluso, la propia LFTR, en sus artículos 190 y 191, estipula la necesidad de proteger los datos que los concesionarios y autorizados recaban de los usuarios en cumplimiento a los Lineamientos.

Asimismo, sería conveniente que el Instituto estableciera, en términos generales, que las autoridades también tienen obligaciones en relación con la protección de estos datos de los usuarios, en los términos que indique la respectiva normatividad en la materia (sea federal o estatal).

A partir de estas consideraciones sobre las facultades del Instituto en protección de datos personales en posesión de los proveedores de servicios de telecomunicaciones y de las opiniones vertidas por el INAI, propuse que se incluyera en los Lineamientos:

1. Un conjunto de medidas de protección de datos que, desde un punto de vista integral, garanticen la protección de la información personal de los usuarios, entre ellas:
    - La creación de políticas internas para la gestión y tratamiento de los datos personales.
    - La identificación de las funciones y obligaciones de las personas que tratan los datos personales.
    - La determinación de las medidas de seguridad aplicables considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser hardware, software, personal del responsable, entre otros.
    - El monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.
    - El diseño y aplicación de diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales, entre otros.
2. La obligación de las autoridades de atender la normatividad aplicable (sea federal o estatal) en materia de protección de datos.

3. Que el tratamiento de los datos personales con motivo de la implementación y operación del número 911 se deberá realizar de conformidad con lo dispuesto en la normatividad que resulte aplicable al sector público federal.

**Problema 10. Se debió incluir una plataforma electrónica única para la solicitud y envío de requerimientos y no varias plataformas, tanto físicas como electrónicas, como lo propone el proyecto.**

La comunicación entre autoridades y los proveedores de servicios de comunicaciones para la transferencia de los registros de geolocalización y de intervención de comunicaciones, debe ser a través de plataformas o **interfaces electrónicas que garanticen la integridad y seguridad de la información transmitida, así como la administración y gestión efectiva del tráfico** entre ambas partes, sin importar el volumen, la duración, y el número de peticiones que realicen múltiples autoridades.

Para ello **es indispensable estandarizar el proceso de requisición y de entrega de los datos que soliciten las autoridades.** Este proceso debe ser capaz de al menos cumplir con las siguientes características:

- Confiabilidad
- Precisión
- Rapidez sin interrupciones
- Seguridad
- Menor costo posible de implementación
- Estandarización de los procesos involucrados

Las interfaces electrónicas deben ser de alta confiabilidad y seguridad. Por lo tanto es recomendable que el IFT establezca en los Lineamientos el deber y no sólo la potestad referente al uso de protocolos y métodos de codificación que garanticen la integridad y seguridad en la transmisión de los datos entre las autoridades y concesionarios. Del mismo modo, es esencial que se genere una plataforma única – y que no se genere una multitud de plataformas o caminos a seguir, como se hace en el Proyecto de Lineamientos- dado que esto último puede causar desorden e incertidumbre sobre si se cumplen o no los estándares mínimos requeridos.

**Problema 11. No se hace un análisis profundo respecto de quién asumirá los costos que se generarán con la colaboración en cuestión.**

Por último, es necesario señalar que no se hace un análisis cabal respecto quién asumirá todos los costos que generará la implementación de toda la colaboración y acciones a tomarse, como consecuencia de los Lineamientos.

### 3. Cuestiones que ameritan un voto diferenciado

Una vez expuesta mi posición respecto a los principales problemas y teniendo en cuenta los argumentos ahí señalados, en el siguiente cuadro hago mención a ciertos considerandos, artículos, capítulos y anexos del Proyecto que no comparto, así como las consideraciones por las cuales me aparto de estos:

| Tabla 4. Consideraciones de mis votos en contra | | |
|---|---|---|
| **Parte del Proyecto en la que voto en contra** | | **Consideraciones** |
| **Considerandos** | Segundo, Tercero y Cuarto Quinto | No comparto lo expresado en estos Considerandos dado que: i) no hacen un análisis exhaustivo del marco nacional e internacional que rige el derecho a la privacidad de los usuarios y protección de sus datos personales, en casos como los previstos por los Lineamientos; ii) no se analiza cómo el Instituto puede crear mecanismos a través de los presentes para garantizar lo anterior; y iii) no contemplan las mejores prácticas internacionales en la materia. |
| **Lineamientos** | 1°, párrafos primero y segundo. | **Voto en contra del lineamiento 1°, párrafos primero y segundo.**<br>En cuanto al párrafo primero, si bien considero que el objetivo es adecuado y acertado como se encuentra redactado, no obstante este objetivo de lograr una oportuna y efectiva colaboración, y de salvaguardar la protección de la privacidad y los datos personales de los usuarios no se logra jurídica ni materialmente en los Lineamientos.<br><br>Lo anterior dado que, para ello era necesario: i) establecer una plataforma única de solicitud y envío de requerimientos como único medio de transmisión de información y con un estándar alto en materia de seguridad de la información; ii) establecer mecanismos de protección efectivos de la privacidad de los usuarios; iii) contemplar un listado de las autoridades que serán consideradas como facultadas; iv) establecer un procedimiento claro, efectivo y exhaustivo de la atención de requerimientos; y v) reconocer que el acceso al registro de datos es una intervención de comunicaciones y, por ello, necesita de previa autorización judicial.<br><br>En cuanto al segundo párrafo, me aparto de éste porque hace mención a los "*proveedores de servicios de aplicaciones y contenidos*". Cuando que, la LFTR en su artículo 190, sólo limita el ámbito de los |

| | | |
|---|---|---|
| | | Lineamientos a los concesionarios y autorizados, y no así a los proveedores de servicios de aplicaciones y contenidos previstos exclusivamente en el artículo 189, primer párrafo, de la LFTR. |
| **Lineamientos** | 2°, fracciones III, XXV, XXVI. | **Voto en contra del lineamiento 2°, fracciones III, XXV, XXVI.**<br>La fracción III establece una definición de autoridades facultadas. Al respecto, me aparto de dicha definición porque considero que un acuerdo delegatorio no puede facultar a una autoridad a requerir los datos o una geolocalización –como lo sugiere la definición- porque, en esta materia, existe una reserva de ley.<br><br>En cuanto a la fracción XXV considero que no es pertinente establecer varios sistemas electrónicos o plataformas electrónicos, sino que, es necesario que sólo exista una plataforma única de alta seguridad de solicitud y envío de requerimientos como único medio de transmisión de información.<br><br>Respecto a la fracción XXVI, no debe contemplarse el Portal de Información como algo "probable" y "eventual", sino que su constitución debería ser obligatoria. También, dicho Portal debería ser administrado o coordinado por el Instituto, esto a efecto de dar mayor certeza a los concesionarios y autoridades y tutelar derechos de usuarios en forma eficaz.<br><br>Al efecto, el Instituto para poder asegurar la eficacia y oportunidad de la colaboración debe incluir a las autoridades en el ecosistema a crear y por tanto tiene la facultad de establecerles normas y procesos obligatorios pues es en su mejor interés al ser usuarias del sistema. Esto en el entendido que en una colaboración –por definición- participan dos o más partes. |
| **Lineamientos** | 3°. | **Voto en contra del lineamiento 3.**<br><br>Me aparto de este lineamiento por la misma razón que ya mencioné relativa al lineamiento 1, segundo párrafo. |
| **Lineamientos** | 4°, 5°, 6°, | **Voto en contra del Capítulo II (lineamientos 4 a 8).** |

| | | |
|---|---|---|
| | 7° y 8° (en su totalidad el Capítulo II). | Me aparto en su totalidad de las disposiciones contenidas en dicho Capítulo, dado que no establecen un sistema claro que permita la efectiva y oportuna colaboración entre los concesionarios y autoridades. Esto, toda vez que se establece una multiplicidad de vías para requerir y entregar la información (incluyendo medios físicos) que no permiten estandarizar y cuidar el procedimiento.<br><br>Las interfaces electrónicas deben ser de alta confiabilidad y seguridad. Por lo tanto es recomendable que el IFT establezca en los Lineamientos **el deber** y no sólo la potestad referente al uso de protocolos y métodos de codificación que garanticen la integridad y seguridad en la transmisión de los datos entre las autoridades y concesionarios. Del mismo modo, es esencial que no se genere una multitud de plataformas o caminos a seguir, dado que eso puede causar desorden e incertidumbre sobre si se cumplen o no los estándares mínimos requeridos. |
| **Lineamientos** | 9°, 10° y 11° (en su totalidad el Capítulo III). | **Voto en contra del Capítulo III (lineamientos 9 a 11).**<br><br>Me aparto en su totalidad de las disposiciones contenidas en dicho Capítulo. Esto, por las razones expuestas respecto al Capítulo anterior y porque, a pesar de que la Geolocalización no necesite autorización judicial, no significa que pueda ser aplicada en todos los casos y de manera indiscriminada. Al respecto, la Suprema Corte de Justicia ha propuesto un estándar a través de la Acción de Inconstitucionalidad 32/2012, en el cual se contempló, entre otras cosas, la procedencia de la geolocalización sin autorización judicial sólo en las investigaciones de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas. Este estándar, que debió ser considerado en los presentes Lineamientos. |
| **Lineamientos** | 12°, 13° y 14° (en su totalidad | **Voto en contra del Capítulo IV (lineamientos 12 a 14).**<br><br>Me aparto en su totalidad de las disposiciones contenidas en dicho Capítulo. Esto, dado que, desde mi |

| | | |
|---|---|---|
| | el Capítulo IV). | perspectiva, en los lineamientos se debería de establecer que, para el **Acceso** al Registro de Datos, sí se necesita autorización judicial. Lo anterior tomando en cuenta: i) los artículos 1, 21, 73 y 89 de la Constitución; 189 y 190 de la LFTR; 34 y 35 de la Ley de Seguridad Nacional; 291 del Código Nacional de Procedimientos Penales; diversos criterios de la Suprema Corte de Justicia de la Nación; los casos *Tristán Donoso vs Panamá*, *Fontevecchia y D´amico vs Argetina*, *Escher y otros vs Brasil*; los Principios internacionales sobre vigilancia de las comunicaciones; y el Reporte del ex -relator especial de la ONU, sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank la Rue.<br><br>Esto en el entendido que el derecho a la privacidad no sólo protege el mensaje que se transmite en la comunicación, sino cualquier dato que pueda identificar el proceso comunicativo, realizado éste a través de cualquier medio o tecnología. |
| **Lineamientos** | 15°, fracciones IV y VI. | **Voto en contra del lineamiento 15°, fracciones I y III.**<br><br>Me aparto de la fracción IV porque considero necesario que no sean diversas plataformas tecnológicas, sino que sólo sea una plataforma única, como ya lo señalé anteriormente.<br><br>Respecto a la fracción VI, voto en contra porque considero que los Grupos de Trabajo no tienen facultades para decidir sobre la "implementación" de nuevos requerimientos de información conforme a la evolución tecnológica de las telecomunicaciones. Estos requerimientos tienen reserva de ley, pues es el legislador el único facultado para implementar o reconocer explícitamente la procedencia de nuevos requerimientos. De este modo, el artículo 190, fracción IV, de la LFTR estipula limitativamente estos tipos de requerimientos, incluso la Ley General de Transparencia y Acceso a la Información se refiere a estos mismos requerimientos en su artículo 70, fracción XLVII. |
| **Lineamientos** | 16°, fracción I. | **Voto en contra del lineamiento 16°, fracción I.**<br><br>Al respecto, considero que el objeto de este Grupo Ejecutivo de Trabajo podría subsumirse en el del Grupo Técnico, dado que el objetivo que se establece no es compatible con otros Lineamientos.. |

| | | |
|---|---|---|
| | | Asimismo, este Grupo Ejecutivo tiene la labor de *"tomar decisiones estratégicas en cuanto a la implementación técnica de los presentes lineamientos"*. De lo anterior se desprende que "implementar" se traduce en "interpretar con efectos vinculantes y definitivos" los presentes Lineamientos. A pesar de que en los presentes lineamientos se establezca que "Los acuerdos alcanzados entre las Autoridades Facultadas y los Concesionarios y Autorizados, en ningún sentido serán vinculantes para el Instituto ni implicarán la modificación de los presentes lineamientos", no veo cómo se puede alcanzar el objetivo si no se realiza una interpretación definitiva de los lineamientos, por lo que me parece contradictorio. |
| **Lineamientos** | 17° y 18° (en su totalidad el Capítulo VI). | **Voto en contra del Capítulo VI (lineamientos 17° y 18°).**<br><br>Me aparto en su totalidad de las disposiciones contenidas en dicho Capítulo. En especial porque hace falta incluir en los Lineamientos dos elementos adicionales: i) la notificación al usuario cuya línea o dispositivo fue objeto de un requerimiento, con posterioridad a éste y ii) que las autoridades facultades proporcionen información estadística sobre colaboraciones o requerimientos que llevaron a investigaciones o prevenciones exitosas. |
| **Anexos** | I y II (en su totalidad los Anexos). | **Voto en contra de los Anexos.**<br><br>Respecto al Anexo I era necesario contemplar diferentes formatos según el tipo de información que se requiriera. Estos tipos de requerimientos están contemplados en el artículo 190, fracción IV, de la LFTR. Incluso, la Ley General de Transparencia y Acceso a la Información se refiere a estos mismos requerimientos en su artículo 70, fracción XLVII.<br><br>En segundo lugar, hace falta contemplar campos adicionales en dichos formatos como los siguientes: i) que se establezca la necesidad y el objetivo que motiva el requerimiento (esto con base en el principio de necesidad), ii) que se justifique por qué el obtener la información requerida es el único medio para alcanzar el objetivo mencionado con anterioridad o que es el menos propenso a vulnerar los derechos humanos (con base en el principio de idoneidad) y 3) que la medida es proporcional con el objetivo |

| | | |
|---|---|---|
| | | que se desea alcanzar (con base en el principio de proporcionalidad).<br><br>En tercer lugar, este Anexo se encuentra relacionado con el lineamiento Cuarto, el cual señala que no es forzoso que las Autoridades Designadas utilicen dicho formato.<br><br>Respecto al Anexo II, me aparto de dicho anexo porque es necesario requerir datos adicionales en dicho formato a los concesionarios y autorizados. Considerando lo dispuesto por el artículo 70, fracción XLVIII de la Ley General de Transparencia, el listado no sólo debe tener el número de solicitudes/requerimientos, sino además: el objeto, el alcance temporal y los fundamentos legales del requerimiento, así como, en su caso, la mención de que cuenta con la autorización judicial correspondiente. |
| **Transitorios** | 2°, párrafos tercero y cuarto. | **Voto en contra del transitorio 2°, párrafos tercero y cuarto.**<br><br>Esto porque ambos párrafos hacen mención a los diversos sistemas electrónicos de los concesionarios y autorizados. No obstante, como ya señalé anteriormente, debería contemplarse en su lugar la creación de una plataforma electrónica única para todos. |
| **Transitorios** | 3°. | **Voto en contra del transitorio 3°.**<br><br>Esto por las mismas razones que el artículo transitorio anterior. |
| **Transitorios** | 4°. | **Voto en contra del transitorio 4°.**<br><br>Esto por las mismas razones que el artículo transitorio anterior. Asimismo, dicho transitorio contempla que un medio a implementar es la página electrónica, en la que se señala que: *"el Concesionario o Autorizado establecerá dicha página electrónica con control de acceso (nombre de usuario y contraseña), para el requerimiento y entrega de información con las Autoridades Designadas."* **Al respecto, este mecanismo de control de acceso es fácilmente vulnerable, pues no se establece un mayor control de acceso a la página electrónica**. No se contempla ni una VPN encriptada, ni enlaces |

| | | |
|---|---|---|
| | | dedicados ni mecanismos efectivos de seguridad y uniformidad. |
| **Transitorios** | 6°. | **Voto en contra del transitorio 6°.**<br><br>Este artículo "faculta" a las autoridades **para establecer por sí mismas o por conducto de Conferencias, los convenios, acuerdos y demás resoluciones encaminadas a facilitar la observancia de los presentes Lineamientos.** Al respecto, voto en contra de dicho artículo porque considero que hace falta señalar que esto no debe propiciar que, por medio de dichos acuerdos o resoluciones, se evadan o modifiquen los presentes Lineamientos. |

Por todo lo anteriormente expuesto, y considerando que los Lineamientos, acuerdos y artículos señalados anteriormente no cumplían con un estándar protector en materia de derechos humanos, que como autoridad debemos garantizar, emití mi votación en los siguientes términos:

| Tabla 5. Votación | |
|---|---|
| **Parte del Proyecto** | **Votación** |
| El Acuerdo en lo General | 1. A favor |
| Considerandos | 2. En contra de los considerandos segundo a quinto. |
| Acuerdo Primero (por el que se emiten los Lineamientos) | 3. En contra de los lineamientos:<br>• 1°, párrafos primero y segundo;<br>• 2°, fracciones III, XXV, XXVI;<br>• 3°;<br>• 4°, 5°, 6°, 7° y 8° (en su totalidad el Capítulo II);<br>• 9°, 10° y 11° (en su totalidad el Capítulo III);<br>• 12°, 13° y 14° (en su totalidad el Capítulo IV);<br>• 15°, fracciones IV y VI;<br>• 16°, fracción I; y<br>• 17° y 18° (en su totalidad el Capítulo VI).<br>4. A favor de los demás lineamientos. |
| Anexos del Acuerdo Primero | 5. En contra de los Anexos I y II (es decir, de la totalidad de los anexos). |
| Acuerdo Segundo | 6. A favor. |
| Transitorios | 7. En contra de los artículos transitorios:<br>• 2°, párrafos tercero y cuarto;<br>• 3°;<br>• 4°;<br>• 6°;<br>8. A favor de los demás artículos transitorios. |

**MÉXICO, DISTRITO FEDERAL,**

**ADRIANA LABARDINI INZUNZA**
**COMISIONADA DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES**