Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México

Por Luis Fernando García
con los aportes de Katitza Rodríguez

Agosto 2016

Luis Fernando García es director de la Red en Defensa de los Derechos Digitales (R3D), abogado egresado de la Universidad Iberoamericana y candidato a Magíster del Programa de Derecho Internacional de los Derechos Humanos de la Universidad de Lund.

Informe preparado en alianza con la Electronic Frontier Foundation. Agradecemos los aportes de Katitza Rodríguez, Directora Internacional de Derechos Humanos por la revisión sustantiva del informe, Kim Carlson y David Bogado de EFF por la corrección de estilo y formato.

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

La Red en Defensa de los Derechos Digitales (R3D) es una organización mexicana dedicada a la defensa de los derechos humanos en el entorno digital.

Índice de contenido

Introducción

El derecho a la privacidad es un derecho esencial para la dignidad humana y para la prevalencia de una sociedad democrática en tanto permite el ejercicio de derechos como la libertad de expresión, libertad de asociación e incluso, el ejercicio del derecho a la salud. No obstante, el derecho a la privacidad se encuentra cada vez más amenazado por actores públicos y privados que buscan aprovechar las posibilidades de interferencia en la vida privada que otorga el avance tecnológico.

Si bien la utilización de la tecnología para la persecución del crimen y/o la protección de la seguridad puede tener un objetivo legítimo, es importante que la consecución de dichos objetivos tome en consideración que al ser medidas altamente invasivas, y además, que suelen requerir de la secrecía para ser efectivas, implique graves riesgos a los derechos humanos.

Es por ello que tanto el derecho internacional de los derechos humanos como la doctrina constitucional de diversos países, han establecido una pluralidad de principios que buscan inhibir los riesgos de abuso y garantizar la rendición de cuentas. Mas aún, la naturaleza secreta de las medidas de vigilancia representan una seria amenaza para la dignidad de las personas y para las aspiraciones de convivencia democrática.

En México, si bien existen protecciones constitucionales y convencionales amplias al derecho a la privacidad, en la última década se han ampliado de manera exponencial las capacidades técnicas y legales para la vigilancia de las comunicaciones. Dicha expansión de facultades no ha venido acompañada de las salvaguardas adecuadas, lo cual, en un país con la debilidad institucional que posee México, representa un grave riesgo a la seguridad de las personas, en particular de grupos vulnerables como los periodistas y los defensores de derechos humanos.

El presente documento desarrolla la protecciones constitucionales e internacionales de los derechos humanos relativos al derecho a la privacidad en los contextos de la vigilancia de las comunicaciones. El texto describe la regulación interna en la materia y formula recomendaciones de reforma legal con base en los estándares de derechos humanos recogidos por los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[1]

I.
Marco jurídico constitucional de la protección de los derechos humanos frente a la vigilancia estatal de las comunicaciones en México

La privacidad de las comunicaciones se encuentra protegida por el artículo 16 de la Constitución. En específico, los párrafos decimosegundo y decimotercero de dicho artículo, contemplan lo que ha sido caracterizado por los órganos de interpretación constitucional en México como el derecho a la inviolabilidad de las comunicaciones:

> *"Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.*
>
> *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. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor."*

De esta forma, la Constitución establece salvaguardas especiales respecto de medidas que interfieran con el derecho a la inviolabilidad de las comunicaciones, como la necesidad de autorización judicial federal para la intervención de comunicaciones privadas; el deber de fundamentación y motivación; y requisitos de claridad respecto de la solicitud como tipo de intervención, sujetos y duración, así como la limitación de autoridades facultadas a únicamente a aquellas autoridades federales que faculte una ley o al titular del Ministerio Público de una entidad federativa.

En la interpretación de este precepto, por ejemplo, al resolver el Amparo en Revisión 1621/2010 y la Contradicción de Tesis 194/2012, la Suprema Corte de Justicia de la Nación

(SCJN) ha establecido que la protección constitucional de las comunicaciones privadas incluye todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, incluidas las formas de comunicación a través de internet.[2]

De igual manera, la SCJN ha señalado explícitamente que la protección constitucional respecto de la inviolabilidad de las comunicaciones puede comprender no sólo el contenido y el proceso de comunicación, sino también 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."*

En atención a este concepto, es que la SCJN ha considerado, por ejemplo, que el acceso y análisis de datos almacenados en un teléfono móvil sin autorización judicial, constituye una violación al derecho a la inviolabilidad de las comunicaciones privadas.[3]

De igual manera, la SCJN ha resuelto recientemente que el acceso a metadatos de comunicaciones conservados por las empresas de telecomunicaciones debe esar precedida de una autorización judicial.[4]

La SCJN ha señalado que la violación al derecho a la inviolabilidad de las comunicaciones se consuma en el momento en que se escucha, graba, almacena, lee o registra, sin el consentimiento de los interlocutores, una comunicación ajena, con independencia de que, con posterioridad, se difunda el contenido de la comunicación interceptada.[5]

Es por ello que, por ejemplo, para la SCJN se considera interceptado un correo electrónico de manera contraria al derecho a la inviolabilidad de las comunicaciones desde el momento en que, sin autorización judicial o consentimiento del titular de una cuenta, se viola la clave

de seguridad (contraseña o password en inglés), con independencia del análisis del contenido de los correos electrónicos.[6]

La SCJN ha interpretado que la protección constitucional a las comunicaciones, en cuanto a su ámbito temporal, se extiende con posterioridad al momento en que la comunicación se produce. De esta forma, la Constitución protege a las personas de interceptaciones de comunicaciones en tiempo real, así como aquellas injerencias que se realizan con posterioridad en los soportes materiales que almacenan la comunicación.[7]

No obstante lo anterior, la SCJN recientemente ha considerado que obligaciones legales impuestas a empresas de telecomunicaciones, consistentes en la conservación obligatoria de metadatos de comunicaciones por dos años, como las que establece la Ley Federal de Telecomunicaciones y Radiodifusión, no constituyen una interferencia en el derecho a la inviolabilidad de comunicaciones privadas.[8]

Asímismo, la SCJN no ha considerado que la protección constitucional otorgada al contenido de las comunicaciones y a algunos metadatos de comunicaciones se extienda a los datos de localización de un teléfono móvil. Un ejemplo de lo anterior es la decisión de la SCJN al resolver la acción de inconstitucionalidad 32/2012,[9] en la que la mayoría de la Suprema Corte consideró que una disposición que faculta a la Procuraduría General de la República (PGR) a monitorear la localización geográfica de un teléfono móvil, en tiempo real, sin necesidad de obtener autorización judicial federal era constitucional.

De lo anterior, se desprende que, si bien, a nivel normativo la Constitución otorga protecciones amplias al derecho a la inviolabilidad de las comunicaciones, la interpretación de esas disposiciones no ha alcanzado a proteger a las personas de las obligaciones de conservación masiva de datos ni la protección de los datos de localización de teléfonos móviles.

I.1 Fuerza normativa de los tratados internacionales en materia de derechos humanos en México que pueden ser afectados por la vigilancia estatal de las comunicaciones

El ordenamiento jurídico mexicano ha sido modificado de manera trascendental en los últimos años, de manera que los derechos humanos han pasado a ocupar un lugar primordial. En particular, la reforma constitucional al artículo primero constitucional y otros, publicada en el Diario Oficial de la Federación el 10 de junio de 2011, introdujo cambios que pretenden profundizar la preponderancia normativa de los derechos humanos.

Uno de los cambios más importantes reflejados en el artículo primero de la Constitución es

el reconocimiento y recepción del derecho internacional de los derechos humanos. Asimismo, la Constitución establece el principio de interpretación más favorable o *principio pro personae*, por el cual, en general, se eliminaría cualquier relación de jerarquía entre las fuentes del derecho que reconocen los derechos humanos.

De igual manera, la reforma constitucional introdujo de manera explícita la obligación de todas las autoridades de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, indivisibilidad, interdependencia y progresividad.

A partir de la reforma constitucional, la SCJN ha desarrollado una doctrina que reconoce a las fuentes del derecho constitucional e internacional de los derechos humanos,[10] como internacional, como integrantes de un mismo catálogo que tanto la autoridad como el orden jurídico mexicano deben respetar.

Lo anterior implica que los derechos humanos reconocidos en la Constitución y en los tratados internacionales como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos, incluyendo la interpretación por parte de sus órganos autorizados, forman parte de un mismo "parámetro de regularidad constitucional" sin que exista jerarquía entre dichas normas. En caso de antinomias, se entiende que, conforme al principio *pro personae* debe preferirse la norma que sea más favorable.

Asimismo, derivado de la reforma constitucional en materia de amparo, publicada el 6 de junio de 2011, se ha consolidado dicho "parámetro de regularidad constitucional", en tanto que ha sido establecida de manera explícita la posibilidad de controlar la constitucionalidad y convencionalidad de toda norma y acto de autoridad a través del juicio de amparo. De esta forma, las personas poseen una poderosa herramienta para combatir violaciones a sus derechos humanos, inclusive en aplicación directa del derecho internacional de los derechos humanos.

I.2 Salvaguardas a la vigilancia estatal de las comunicaciones en el derecho internacional

En el Derecho Internacional de los Derechos Humanos también se ha desarrollado el contenido y alcance del derecho a la privacidad en contextos de vigilancia.

En el Sistema Interamericano de Derechos Humanos, si bien no existe una cantidad importante de decisiones sobre el tema, se encuentran algunos precedentes ampliamente protectores del derecho a la privacidad de las comunicaciones. Por ejemplo, en el *Caso Escher vs. Brasil*, la Corte Interamericana de Derechos Humanos (Corte IDH) ha

interpretado el artículo 11 de la Convención Americana sobre Derechos Humanos (CADH), que reconoce el derecho a la no injerencia arbitraria en las comunicaciones, en el sentido de que este protege tanto el contenido de las comunicaciones como los *metadatos* que identifican dicha comunicación:

> *"[E]l artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación."*

De esta forma se confirma el criterio adoptado por el Poder Judicial mexicano, en el sentido que no sólo el contenido de las comunicaciones se encuentra protegido por el parámetro de regularidad constitucional, sino que además, cualquier elemento del proceso comunicativo, es decir, los *metadatos*, también poseen protección constitucional y convencional.

Por otro lado, tanto la Comisión Interamericana de Derechos Humanos, a través de la Relatoría Especial para la Libertad de Expresión, como el Relator Especial de Naciones Unidas sobre la promoción y protección del derecho a la libertad de expresión y opinión han indicado la importancia de la adopción de salvaguardas adecuadas para inhibir los riesgos de abuso de las medidas de vigilancia de las comunicaciones, en tanto constituyen interferencias severas con el derecho a la privacidad y el derecho a la libertad de expresión.

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

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

autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación."[11]

De igual manera, los mecanismos internacionales de protección mencionados han señalado que en el contexto de medidas de vigilancia encubierta, la ley debe ser lo suficientemente clara en sus términos para otorgar a los ciudadanos una indicación adecuada respecto de las condiciones y circunstancias en que las autoridades están facultadas para recurrir a dichas medidas.[12]

Además, en vista del riesgo de abuso que cualquier sistema de vigilancia secreta implica, las medidas deben basarse en una ley que sea particularmente precisa, en vista de que la tecnología disponible para realizar esas actividades continuamente se vuelve más sofisticada.[13] Es por ello que para que las medidas de vigilancia encubierta cumplan con el *examen de necesidad* de restricciones al derecho a la privacidad, es fundamental que existan medidas para inhibir los riesgos inherentes de abuso.

Organismos de protección internacional de derechos humanos como el Tribunal Europeo de Derechos Humanos han resaltado en su jurisprudencia reiterada que la existencia de salvaguardas adecuadas y efectivas son fundamentales para que se cumpla el criterio de necesidad y proporcionalidad proscrito en las legislaciones que le facultan invasiones a la privacidad.[14]

En consonancia, la relevancia de garantías efectivas en contra del abuso de medidas de vigilancia electrónica encubierta ha sido destacada recientemente por la Asamblea General de la Organización de las Naciones Unidas (ONU),[15] el Relator Especial de la ONU para el Derecho a la Libertad de Expresión y Opinión,[16] la Alta Comisionada para los Derechos Humanos de la ONU,[17] la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos,[18] así como por organizaciones de la sociedad civil y expertos que han recogido las mejores prácticas derivadas de la jurisprudencia y doctrina comparada y han elaborado los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[19]

Una de las salvaguardas fundamentales para inhibir los riesgos inherentes de abuso de las medidas de vigilancia es el control judicial. La relevancia fundamental del control judicial previo o inmediato de medidas de vigilancia encubierta que invaden la privacidad de las personas ha sido resaltada recientemente por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, la cual ha señalado que:

"Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida

es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover."[20]

Otras de las medidas identificadas en el derecho internacional como salvaguardas adecuadas para inhibir abusos en la implementación de medidas de vigilancia encubierta de comunicaciones son la existencia de mecanismos de supervisión independiente y la transparencia estadística de medidas de vigilancia.

Por ejemplo, en la resolución "El derecho a la privacidad en la era digital", adoptada por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013, se recomienda a los Estados establecer o mantener "mecanismos nacionales de supervisión independiente y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado."[21]

A su vez el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas ha expresado en su Informe las consecuencias de la vigilancia de las comunicaciones:

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

Los Estados deben otorgar a los individuos suficiente información para permitirles comprender totalmente el alcance, naturaleza y aplicación de leyes que permiten la vigilancia de comunicaciones. Los Estados deben permitir a los proveedores de servicios la publicación de los procedimientos que aplican para manejar la vigilancia de comunicaciones estatal, adherirse a esos procedimientos, y publicar registros sobre la vigilancia de comunicaciones estatal. (...)"[22]

De igual manera en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto para la Libertad de Expresión[23] del Relator Especial sobre el Derecho a la Libertad de Opinión y expresión de la ONU y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos (CIDH) han señalado que:

> *"Toda persona tiene derecho a acceder a información bajo el control del Estado. Este derecho incluye la información que se relaciona con la seguridad nacional, salvo las precisas excepciones que establezca la ley, siempre que estas resulten necesarias en una sociedad democrática. Las leyes deben asegurar que el público pueda acceder a información sobre los programas de vigilancia de comunicaciones privadas, su alcance y los controles existentes para garantizar que no puedan ser usados de manera arbitraria. En consecuencia, los Estados deben difundir, por lo menos, información relativa al marco regulatorio de los programas de vigilancia; los órganos encargados para implementar y supervisar dichos programas; los procedimientos de autorización, de selección de objetivos y de manejo de datos, así como información sobre el uso de estas técnicas, incluidos datos agregados sobre su alcance. En todo caso, los Estados deben establecer mecanismos de control independientes capaces de asegurar transparencia y rendición de cuentas sobre estos programas. (...)*
>
> *El Estado tiene la obligación de divulgar ampliamente la información sobre programas ilegales de vigilancia de comunicaciones privadas. Esta obligación debe ser satisfecha sin perjuicio del derecho a la información personal de quienes habrían sido afectados. En todo caso, los Estados deben adelantar investigaciones exhaustivas para identificar y sancionar a los responsables de este tipo de prácticas e informar oportunamente a quienes han podido ser víctima de las mismas."*

Lo anterior ha sido reiterado por la Relatora Especial para la Libertad de Expresión de la CIDH la cual señaló en su "Informe sobre Libertad de Expresión e Internet"[24] que:

> *"Los Estados deberían publicar información global sobre el número de solicitudes de intercepción y vigilancia aprobadas y rechazadas, incluyendo la mayor cantidad de información posible como – por ejemplo – un desglose de solicitudes por proveedor de servicios, tipo de investigación, tiempo durante el cual se extienden las investigaciones, etcétera."*

Otro instrumento que reconoce la obligación de los Estados de garantizar la transparencia respecto de programas de vigilancia para fines de seguridad nacional son los Principios Globales sobre Seguridad Nacional y Derecho a la Información (Principios de Tshwane)[25] los cuales señalan en su Principio 10 "Categorías de información sobre las cuales existe una fuerte presunción o un interés esencial a favor de su divulgación":

> *"E. Vigilancia*
>
> *(1) El público debería conocer tanto las leyes y principales reglamentaciones a todas las formas de vigilancia secreta como los procedimientos relativos a la autorización de dicha vigilancia, la selección de objetivos, el uso, intercambio, almacenamiento y la destrucción y el material interceptado.*
>
> *(2) El público también deber tener acceso a la información sobre las entidades autorizadas para llevar a cabo acciones de vigilancia, y a las estadísticas relativas al uso de dichas acciones.*
>
> *(3) Se debería informar al público, además, de las vigilancias ilegales. La información acerca de este tipo de vigilancias debería ser hecha pública en la mayor medida posible, sin violar los derechos de privacidad de las personas vigiladas.*
>
> *(4) Estos Principios abordan el derecho del público a acceder a la información y se entienden sin perjuicio a los derechos sustantivos y procesales adicionales de los individuos que han sido, o creen haber sido, sujetos a vigilancia."*

Por su parte, otra de las salvaguardas adecuadas para garantizar la necesidad y proporcionalidad de las medidas de vigilancia es el derecho de notificación al afectado. Este derecho de notificación a las personas afectadas por medidas de vigilancia ha sido reconocido, por ejemplo, por el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas:

> *"Los individuos deben contar con el derecho a ser notificados que han sido sujetos de medidas de vigilancia de sus comunicaciones o que sus comunicaciones han sido accesadas por el Estado. Reconociendo que la notificación previa o concurrente puede poner en riesgo la efectividad de la vigilancia, los individuos deben ser notificados, en cualquier caso, una vez que la vigilancia ha sido completada y se cuenta con la posibilidad de buscar la reparación que proceda respecto del uso de medidas de vigilancia de las comunicaciones"*[26]

Este derecho de notificación ha sido reconocido, además, por el Tribunal Europeo de Derechos Humanos, el cual determinó en el *Caso Ekimdzhiev vs. Bulgaria* que una vez que la vigilancia ha cesado y ha transcurrido el tiempo estrictamente necesario para que el propósito legítimo de la vigilancia no sea puesto en riesgo, la notificación al afectado debe llevarse a cabo sin dilación.[27]

De esta forma, en el Derecho Internacional de los Derechos Humanos se han desarrollado

estándares de legalidad, idoneidad, necesidad y proporcionalidad para la adopción de medidas de vigilancia que invaden de manera encubierta las comunicaciones privadas.

II.
Normativa de rango legal que aborda la regulación de actividades de vigilancia estatal de las comunicaciones en México

En la legislación federal mexicana, existen múltiples autoridades facultadas para solicitar la intervención de comunicaciones privadas y, en general, llevar a cabo medidas de vigilancia encubierta.

Marco Institucional - Autoridades con Facultades de Intervención de Comunicaciones Privadas en México	
Procuraduría General de la República (Fiscalía General de la Nación) + Procuradurías / Fiscalías de las 31 entidades federativas y el Distrito Federal.	El artículo 16 constitucional establece que los ministerios públicos pueden intervenir comunicaciones privadas, para la investigación de delitos, previa aprobación de la autoridad judicial federal. El Código Federal de Procedimientos Penales y los 32 códigos procesales penales locales, que serán sustituidos por el Código Nacional de Procedimientos Penales permite a los ministerios públicos, además de la intervención de comunicaciones privadas, ordenar la conservación de datos, obtener la localización geográfica en tiempo real de equipos de comunicación, sin autorización judicial, así como acceder a metadatos de comunicaciones.
	Artículo 16 de la Constitución. Código Nacional de Procedimientos Penales (Arts. 291 – 303). Código Federal de Procedimientos Penales (Arts. 278 Bis - 278 Ter). Códigos Procesales Penales locales (31 Estados + Distrito Federal). Ley Federal de Telecomunicaciones y Radiodifusión (Arts. 189 – 190). Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro (Art. 24). Ley Federal contra la Delincuencia Organizada (Arts. 15 – 28).
Comisión Nacional de Seguridad (Policía Federal)	La Ley de la Policía Federal otorga facultades de vigilancia de comunicaciones a la Policía Federal, para la prevención del delito, exclusivamente, cuando exista autorización judicial federal que constate que existen indicios suficientes que acrediten que se está organizando la comisión de ciertos delitos detallados en el artículo 51 de la Ley.
	Ley de la Policía Federal (Arts. 48 – 55). Ley Federal de Telecomunicaciones y Radiodifusión (Arts. 189 – 190).
Centro de Investigación y Seguridad Nacional (Poder Ejecutivo)	La Ley de Seguridad Nacional faculta al Centro de Investigación y Seguridad Nacional para intervenir comunicaciones privadas, previa autorización judicial federal, en casos de "amenaza inminente" a la seguridad nacional.
	Ley de Seguridad Nacional (Arts. 33 – 49). Ley Federal de Telecomunicaciones y Radiodifusión (Arts. 189 – 190).

No obstante lo anterior, en Julio del 2015, ha sido revelado, a través de la publicación de documentos internos de la empresa italiana Hacking Team S.rl., que numerosas autoridades mexicanas, federales y estatales, han adquirido software malicioso de espionaje, la mayoría de ellas, sin facultades constitucionales[28] o legales para intervenir comunicaciones privadas.[29]

II.1 Regulación de la vigilancia estatal de las comunicaciones para prevenir e investigar delitos

En México, la investigación de delitos se encuentra confiada a la Procuraduría General de la República (PGR), así como a las procuradurías de cada una de las 32 entidades federativas. La Procuraduría General de la República (PGR) posee facultades para llevar a cabo diversas medidas de vigilancia encubierta según lo señala el Código Federal de Procedimientos Penales (CFPP) reformado en el año 2009.[30]

El CFPP, que aún se encuentra en vigor a nivel federal, señala en su artículo 278 Bis que "[l]as empresas concesionarias y permisionarias del servicio de telecomunicaciones o de internet, estarán obligadas a colaborar con las autoridades para la obtención de [comunicaciones privadas] cuando así lo soliciten". Igualmente, el artículo 278 Ter detalla el procedimiento a seguir para llevar a cabo la intervención de comunicaciones privadas. Dicho artículo señala la necesidad de obtención de una autorización judicial, la cual será otorgada cuando "se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves".

Además, el CFPP establece que la solicitud, y en su caso la autorización, deben detallar aspectos de la intervención que se pretende llevar a cabo, como lo son: los preceptos legales en los que se funda, el razonamiento por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos, el periodo durante el cual se llevarán a cabo las intervenciones (el cual no debe exceder de seis meses). El juez debe verificar periódicamente el cumplimiento de los términos de la autorización y en caso de que se decrete el no ejercicio de la acción penal, las comunicaciones obtenidas deben ser presentadas ante éste y ser destruidas en su presencia.

Igualmente, las leyes en materia de secuestro expedidas en el año 2010[31] y de delincuencia organizada en 2007[32] otorgan a la PGR la posibilidad de intervenir comunicaciones privadas. Las agencias de procuración de justicia de cada uno de los 31 Estados mexicanos y del Distrito Federal normalmente también poseen facultades de intervención de comunicaciones privadas de conformidad con la legislación estatal.

Asimismo, el artículo 133 Quáter del CFPP establece la posibilidad que la PGR tenga la posibilidad de solicitar a los concesionarios o permisionarios del servicio de telecomunicaciones, por simple oficio o medios electrónicos datos de geolocalización en

tiempo real. Es decir, el CFPP permite otorgar los datos de localización geográfica, en tiempo real, de equipos de comunicación móvil sin autorización judicial, cuando se trate de investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas.

La constitucionalidad de dicho artículo fue combatida a través de la Acción de Inconstitucionalidad 32/2012, interpuesta por la Comisión Nacional de los Derechos Humanos, sin embargo, una mayoría de la SCJN consideró la figura como constitucional, a través de una interpretación conforme basada en el entendimiento de que la figura únicamente se facultaba para casos de emergencia, respecto de delitos específicos y siendo esta localización geográfica una medida efímera, es decir, que se agota en un mismo momento y no permite el monitoreo continuado de los datos de localización.

No obstante lo anterior, en marzo de 2014 fue publicado el Código Nacional de Procedimientos Penales (CNPP), el cual pretende sustituir el Código Federal de Procedimientos Penales, los 31 Códigos Estatales y el Código del Distrito Federal. Dicho Código Nacional entrará en vigor de manera gradual en las diversas entidades federativas y a nivel federal a más tardar en junio de 2016. En el CNPP se reiteran las facultades de vigilancia de las instancias de procuración de justicia contenidas en el Código Federal, aunque con algunas modificaciones.

El artículo 291 del Código Nacional, por ejemplo, deja claro que la intervención de comunicaciones privadas, y la necesidad de obtención de autorización judicial, comprende no sólo el contenido de las comunicaciones, sino también los datos que identifican la comunicación o *metadatos*, ya sea en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo.

No obstante, el Código Nacional de Procedimientos Penales es menos claro que el Código Federal de Procedimientos Penales en cuanto se refiere a la procedencia de la solicitud únicamente cuando existan indicios de participación o causa probable.

En el artículo 303 del CNPP, persiste la posibilidad de monitoreo de la localización geográfica en tiempo real de dispositivos de comunicación sin autorización judicial y se amplía esta posibilidad a cualquier investigación y no a una lista cerrada de delitos como lo establece el CFPP.

La constitucionalidad de dicho artículo será analizado al resolverse las Acciones de Inconstitucionalidad 10/2014 y 11/2014, interpuestas por la CNDH y el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) próximas a resolverse. Esta decisión puede producir un precedente distinto del ya emitido en la Acción de Inconstitucionalidad 32/2012 a la que se ha hecho referencia, en tanto la disposición del CNPP modifica y amplía

de manera sustancial el alcance de la medida por lo que las consideraciones ya esgrimidas por la SCJN no resultan ser aplicables del todo.

Por otro lado, en el CNPP se incluye la posibilidad de ordenar la conservación de datos contenidos en redes, sistemas o equipos de informática sin orden judicial, además que tampoco adiciona salvaguardas adecuadas como la supervisión independiente, medidas de transparencia estadística o mecanismos de notificación diferida al usuario afectado.

En el mes de diciembre del año 2014, el Senado de la República aprobó una reforma a los artículos 291 y 303 del CNPP de manera que se establece de manera inequívoca la necesidad de autorización judicial federal para llevar a cabo la localización geográfica, en tiempo real, de equipos de comunicación móvil y el acceso a datos conservados por concesionarios de telecomunicaciones y proveedores de aplicaciones y servicios en Internet. Dicha reforma aún requiere aprobación de la Cámara de Diputados, la cual se encuentra pendiente.[33]

Por otra parte, las leyes contemplan a autoridades federales distintas de las de procuración de justicia como facultadas para llevar a cabo medidas de vigilancia encubierta.

En el año 2009 fue expedida la Ley de la Policía Federal, la cual faculta a esta dependencia a llevar a cabo la intervención de comunicaciones privadas para la prevención de ciertos delitos.[34] El artículo 48 de dicha ley de manera expresa señala que la autorización judicial para la intervención de comunicaciones privadas podrá otorgarse "únicamente a solicitud del Comisionado General, cuando se constate la existencia de indicios suficientes que acrediten que se está organizando la comisión de [...] delitos" que se listan en el artículo 51 de la ley.

Asímismo, el artículo 8, fracción XXVIII de la ley mencionada, faculta a la Policía Federal a solicitar, previa autorización judicial, a los concesionarios, permisionarios, operadoras telefónicas y todas aquellas comercializadoras de servicios en materia de telecomunicaciones, cualquier información, incluyendo la georreferenciación de los equipos de comunicación móvil en tiempo real, para fines de prevención del delito.

II.2 Regulación de la vigilancia de las comunicaciones en la normativa de telecomunicaciones

Como muchas de las comunicaciones entre las personas se llevan a cabo a través de servicios suministrados por empresas privadas (de telefonía o de internet), muchas veces el Estado requiere de su colaboración para realizar la vigilancia. Esto aplica tanto para el caso de las investigaciones penales como para la protección de la seguridad mediante la realización de actividades de inteligencia.

En este sentido, en el año 2009 fue reformada la Ley Federal de Telecomunicaciones[35] para imponer a las empresas que prestan servicios de telecomunicaciones, la obligación de conservar *metadatos* como el tipo de comunicación, los servicios empleados, el origen y destino de las comunicaciones, fecha, hora y duración de las comunicaciones e incluso la ubicación geográfica de los dispositivos de comunicación. La obligación de conservación de datos posee una duración de doce (12) meses y aplica a todos los usuarios de los servicios prestados por las empresas de telecomunicaciones.

La Ley Federal de Telecomunicaciones permitía a la Procuraduría General de la República y a los procuradores de las entidades federativas el acceso a los datos retenidos por las empresas de telecomunicaciones para la investigación de delitos graves sin que se establezca la necesidad de obtener autorización judicial.

En el año 2014, la Ley Federal de Telecomunicaciones fue sustituida por la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), la cual incrementa de manera considerable las facultades de vigilancia de las autoridades y las obligaciones de colaboración que las empresas que prestan servicios de telecomunicaciones deben brindar a las autoridades para la vigilancia estatal de las comunicaciones.

En su artículo 189, la LFTR establece de manera genérica la obligación de los concesionarios de telecomunicaciones, e incluso, de los proveedores de servicios, aplicaciones y contenidos de "atender todo mandamiento por escrito, fundado y motivado de la autoridad competente", dentro de las cuales se mencionan "las instancias de seguridad y procuración de justicia" sin que se establezca claramente que autoridades comprenden dichas categorías.

Este artículo ha sido considerado por varias autoridades como suficiente habilitación para utilizar herramientas de vigilancia encubierta, sin la necesidad de que dicha facultad esté detallada en otra ley. Por ejemplo, la "Unidad de Inteligencia Financiera" de la Secretaría de Hacienda y Crédito Público se considera una "instancia de seguridad" a partir del mencionado artículo 189 y de un instrumento que no constituye una ley formal y material, a saber, las "Bases de Colaboración que en el marco de la Seguridad Nacional celebran la Secretaría de Gobernación y la Secretaría de Hacienda y Crédito Público".[36] Inclusive, existen reportes de que autoridades como el Instituto Nacional Electoral habría enviado este tipo de solicitudes de acceso a datos personales de usuarios de telecomunicaciones[37]

Similarmente, el artículo 190 fracción I de la LFTR, por su parte, establece la obligación de concesionarios de "colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil". Lo anterior, podría suponer la ampliación de las facultades de "geolocalización" a autoridades que previamente, y actualmente, no poseen esta facultad en una ley habilitante como lo son las "instancias de seguridad" o las "instancias de administración de justicia", las

cuales no se encuentran definidas ni en la LFTR, ni en otra ley.

No obstante lo anterior, la SCJN recientemente ha establecido que para que las autoridades puedan considerarse facultadas para llevar a cabo medidas de vigilancia electrónica, es necesario que las mismas posean autorización expresa en la ley que regule su actuación. De esta manera, la SCJN ha aclarado que las únicas autoridades que se encuentran facultadas son los Ministerios Públicos, la Policía Federal y el Centro de Investigación para la Seguridad Nacional (CISEN).[38]

En el artículo 190 fracción II de la LFTR se establece la obligación de conservar datos de usuarios de telecomunicaciones. Si bien dicha facultad ya existía desde el año 2009 cuando fue incorporada a la ahora abrogada Ley Federal de Telecomunicaciones, el artículo 190 de la LFTR amplía el periodo de retención a 24 meses.

La obligación de los concesionarios de telecomunicaciones consiste de manera puntual en conservar los siguientes datos:

> *a) Nombre, denominación o razón social y domicilio del suscriptor;*
>
> *b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);*
>
> *c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;*
>
> *d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;*
>
> *e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;*
>
> *f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;*
>
> *g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y*
>
> *h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.*

El concesionario debe conservar los datos durante los primeros 12 meses "en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos." Después de lo cual deben conservarse los datos por 12 meses adicionales y ser entregados a la autoridad que lo solicite dentro de las 48 horas siguientes a la solicitud.

A su vez, el artículo 190 fracción III de la LFTR establece la obligación de entregar los datos conservados a "las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran". Como ha sido mencionado anteriormente, la figura de "instancias de seguridad" es sumamente ambigua, aunque la interpretación de la SCJN ha acotado considerablemente su aplicación.

El Instituto Federal de Telecomunicaciones (IFT), de acuerdo al mandato que establece el artíulo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión, expidió los "Lineamientos de Colaboración en materia de Seguridad y Justicia".[39] Si bien prácticamente no se subsanan los vicios de constitucionalidad de la ley, se reconocen algunas salvaguardas en materia de Transparencia.

En concreto, los Lineamientos Décimo Séptimo y Décimo Octavo de los lineamientos señalan lo siguiente:

> *DÉCIMO SÉPTIMO.- Sin perjuicio de lo establecido en la LFTR, los Concesionarios y los Autorizados son responsables respecto a la posesión, protección, tratamiento y control de los Datos Personales de los particulares. Se prohíbe la utilización de los datos conservados tanto para fines distintos a los previstos en el Capítulo Único del Título Octavo de la LFTR, como de los presentes Lineamientos. Cualquier uso distinto será sancionado por las autoridades competentes conforme a la legislación aplicable.*
>
> *DÉCIMO OCTAVO.- Los Concesionarios y Autorizados deberán entregar al Instituto, en el mes de enero y julio de cada año, un informe semestral electrónico a través del mecanismo que para tales efectos establezca el Instituto, relativo al cumplimiento de los presentes Lineamientos. Dicho informe deberá contener y observar lo siguiente:*
>
> *I. El número total y por Autoridad Facultada, de requerimientos de información de localización geográfica en tiempo real y de registro de datos de comunicaciones, desglosando las recibidas, entregadas y no entregadas mensualmente, utilizando el formato que se anexa a los presentes Lineamientos como Anexo II.*

II. En el mes de julio, deberán integrar, además, el informe referido en el lineamiento OCTAVO, fracción VI.

III. En el mes de enero, deberán integrar, además, el informe referido en el lineamiento CUADRAGÉSIMO.

El Instituto solicitará a las Autoridades Designadas y/o Facultadas en el mes de enero y julio de cada año, un informe semestral relativo al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, así como el número de registros de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido el fin para el cual fueron solicitados.

En términos de lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables, las autoridades señaladas en los artículos 189 y 190 de la LFTR, están obligadas a adoptar las medidas necesarias que garanticen la seguridad de los Datos Personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

La información estadística contenida en los informes semestrales será publicada en el portal de Internet del Instituto en términos de lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables.

En términos de lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables, en caso de que los sistemas de conservación de datos hayan sido vulnerados y los Datos Personales de los usuarios finales se encuentren comprometidos, los Concesionarios y Autorizados deberán notificar inmediatamente a éstos e indicar las medidas que el usuario podrá tomar para disminuir o contrarrestar cualquier afectación derivada de esta vulneración.

En un sentido similar, el Congreso de la Unión aprobó en Abril del año 2015 la Ley General de Transparencia y Acceso a la Información Pública. La cual incluye las siguientes obligaciones de transparencia en materia de vigilancia:

Artículo 70. En la Ley Federal y de las Entidades Federativas se contemplará que los sujetos obligados pongan a disposición del público y mantengan actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan:

XLVII. Para efectos estadísticos, el listado de solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de Internet para la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, que contenga exclusivamente 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.

II.3 Regulación de la vigilancia estatal de las comunicaciones en la legislación referida a actividades de inteligencia y contrainteligencia

Aparte de las normas relativas a la prevención e investigación de delitos y las normas de telecomunicaciones, los legisladores contemplaron la posibilidad de restringir los derechos de las personas a través de medidas de vigilancia de comunicaciones en el marco de las actividades de inteligencia y contrainteligencia.

La Ley de Seguridad Nacional también otorga al Centro de Investigación y Seguridad Nacional (CISEN) la facultad de intervenir comunicaciones privadas en casos de "amenaza inminente a la seguridad nacional".[40] El artículo 5 de la Ley define las "amenazas a la seguridad nacional" de una manera sumamente amplia:

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.

Además de las ambigüedades respecto de las circunstancias en las que medidas de vigilancia encubierta pueden ser autorizadas, y si bien, tanto en el caso de la Policía Federal como del CISEN se reconoce la necesidad de autorización judicial federal para llevar a cabo estas medidas, en dichos ordenamientos no se establecen otras salvaguardas contra el abuso como la supervisión de un órgano independiente, obligaciones de transparencia estadística o mecanismos de notificación posterior al afectado por una medida de vigilancia.

Inclusive, en el caso de la seguridad nacional, la ley restringe el acceso a la información en esa materia de manera amplia y vaga. En concreto, el artículo 51 de la Ley de Seguridad Nacional establece como información reservada "aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen", así como "aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza".

De esta forma, los contrapesos institucionales capaces de fiscalizar a las instancias de seguridad nacional son sumamente escasos, lo cual incrementa los riesgos de abuso de poder.

II.4 Recursos jurídicos y sanciones contra el abuso de medidas de vigilancia estatal

El Juicio de Amparo, regulado en la Ley de Amparo, es el recurso adecuado para remediar violaciones a derechos humanos reconocidos, tanto en la Constitución como en las normas de derechos humanos de fuente internacional. En este sentido, es posible utilizar este medio para impugnar actos o normas que vulneren el derecho a la privacidad y a la inviolabilidad de las comunicaciones privadas.

No obstante lo anterior, persisten algunos obstáculos para la plena efectividad del juicio de amparo. Por ejemplo, la Constitución y la Ley de Amparo regulan este juicio de manera que los efectos del mismo solamente tienen efectos particulares, es decir, solamente protegen a la persona que acude al amparo, por lo tanto, en el caso de las normas de vigilancia que no cumplen con los estándares de protección del derecho a la privacidad, la eventual sentencia de amparo solamente protege al demandante y no a la población en general.

Igualmente, persisten algunas decisiones judiciales que no reconocen la legitimación procesal para impugnar normas que establecen medidas de vigilancia de comunicaciones, en tanto se interpreta, que es necesario probar la aplicación de dicha norma al demandante, de manera que pueda demostrar una afectación actual y real.

Dada la naturaleza secreta de las medidas de vigilancia encubierta resulta prácticamente imposible poder probar la aplicación de medidas de vigilancia abusivas. No obstante, se han logrado construir algunos precedentes en donde se reconoce la legitimación de cualquier persona para impugnar medidas de vigilancia encubierta, aún sin probar un acto de aplicación concreto, en tanto se reconoce que dichas normas, por su mera existencia afectan la esfera jurídica de las demandantes.[41]

Por su parte, la Ley Federal de Protección de Datos Personales en Posesión de Particulares, al reconocer los derechos de Acceso, Rectificación, Cancelación y Oposición, otorga algunos mecanismos para que una persona pueda proteger su derecho a la protección de datos personales frente a particulares. La ley contempla un procedimiento de verificación, por medio del cual, el Instituto Nacional de Acceso a la Información y Protección de Datos (INAI) puede verificar el cumplimiento de la ley e imponer sanciones por su incumplimiento.

Finalmente, debe mencionarse que el artículo 177 del Código Penal Federal establece como delito grave, meritorio de una pena de seis a doce años de prisión, la intervención de comunicaciones privadas sin autorización de autoridad judicial competente. Sin embargo, en México no existen precedentes públicos de la aplicación de dicho tipo penal a persona alguna.

III.
¿Respeta la legislación Mexicana los estándares internacionales de derechos humanos en materia de actividades de vigilancia estatal? Algunas propuestas de mejora

Los más altos estándares de protección del derecho a la privacidad en relación con la vigilancia estatal de las comunicaciones, reconocidos de la jurisprudencia y doctrina de los órganos de protección internacional de derechos humanos y de tribunales constitucionales alrededor del mundo, han sido recogidos para elaborar los "Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones".[42]

Los trece principios que en dicho instrumento se desarrollan son:

Legalidad

Cualquier limitación a los derechos humanos debe ser prescrita por ley. La Ley debe ser pública y cumplir un estándar de claridad y precisión suficientes para prever el alcance de las medidas de vigilancia de comunicaciones.

Objetivo Legítimo

Las leyes que establezcan medidas de vigilancia de las comunicaciones deben perseguir objetivos legítimos y no ser aplicadas de manera discriminatoria.

Necesidad

La vigilancia de las comunicaciones sólo debe llevarse a cabo cuando la consecución del objetivo legítimo no pueda alcanzarse a través de métodos menos lesivos a los derechos humanos. La carga de demostrar dicha justificación le corresponde al Estado.

Idoneidad

Las medidas de vigilancia de comunicaciones deben ser apropiadas y capaces de conseguir el objetivo legítimo perseguido.

Proporcionalidad

Las medidas de vigilancia sólo deben autorizarse por una autoridad judicial independiente cuando exista un alto grado de probabilidad de que un delito grave o una amenaza específica, actual y comprobable a la seguridad nacional pueda materializarse. Las medidas de vigilancia adoptadas deben ser las menos invasivas posibles, lo cual implica que solamente se obtendrá, retendrá o utilizará la información relevante para la consecución del objetivo legítimo que justifica la autorización y por periodos de tiempo limitados.

Autoridad Judicial Competente

Las medidas de vigilancia de comunicaciones deben ser autorizadas de manera previa, o inmediata con efecto retroactivo en casos de emergencia, por una autoridad judicial competente, independiente e imparcial.

Debido Proceso

Las decisiones de autorización de medidas de vigilancia de comunicaciones deben garantizar el debido proceso. Lo anterior implica que, cuando para la consecución del objetivo legítimo, y en particular, la protección de la vida de una persona, sea necesaria la secrecía de la medida o su aplicación inmediata, existan otras medidas que garanticen la protección de los intereses del afectado como lo es la designación de una persona o institución que asuma representación general de sus intereses en la audiencia o que la autorización judicial se lleve a cabo con efecto retroactivo.

Notificación del Usuario

Las personas afectadas por medidas de vigilancia de comunicaciones deben ser notificadas de ello y tener acceso a las materiales que pretendan ser o hayan sido obtenidos. La notificación podrá diferirse cuando la misma ponga en riesgo la consecución del objetivo legítimo o exista un riesgo inminente de peligro a la vida humana.

Transparencia

El Estado debe publicar de manera periódica información estadística sobre las medidas de vigilancia encubierta llevadas a cabo. Como mínimo debe publicar el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad, tipo y propósito.

Supervisión Pública

Deben establecerse mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones. Dichos mecanismos de supervisión independiente deben tener la autoridad para acceder a toda la información potencialmente relevante para evaluar el uso legítimo de medidas de vigilancia

de comunicaciones.

Integridad de las Comunicaciones y Sistemas

No debe obligarse a proveedores de servicios o desarrolladores de "hardware" o "software" a desarrollar capacidades de vigilancia que comprometan la seguridad de las comunicaciones y los dispositivos. No debe exigirse la retención indiscriminada y masiva de datos de las personas que usan dichos servicios ni debe comprometerse el derecho a la expresión anónima a través del establecimiento de obligaciones de identificación o prohibiciones respecto del uso de herramientas de cifrado y otras para proteger la identidad y la seguridad de las personas, sus comunicaciones y sus dispositivos.

Garantías para la Cooperación Internacional

Si para llevar a cabo las medidas de vigilancia es necesaria la cooperación internacional, esta debe llevarse a cabo a través de acuerdos de asistencia judicial recíproca (MLAT en inglés) en los que debe garantizarse que los mismos no sean utilizados para burlar las restricciones internas relacionadas con la vigilancia de las comunicaciones.

Garantías contra el Acceso Ilegítimo y Recurso Efectivo

La vigilancia ilegal de comunicaciones por parte de actores públicos o privados debe ser castigada mediante sanciones civiles y penales suficientes y adecuadas. Los denunciantes de información de interés público (whistleblowers en inglés) deben ser protegidos por la ley de cualquier repercusión legal por el incumplimiento de su deber de secrecía.

IV.
Recomendaciones

La legislación que regula la vigilancia de las comunicaciones en México que ha sido desarrollada en el capítulo anterior, no cumple con los estándares de derechos humanos de fuente constitucional e internacional que recogen los 13 Principios mencionados. Por ello, es indispensable que se adopten, como mínimo, las siguientes reformas legales:

IV.1 Vigilancia Estatal de Comunicaciones para la Procuración de Justicia

El Código Nacional de Procedimientos Penales reconoce que la intervención de comunicaciones privadas debe contar con una autorización judicial federal, incluyendo para obtener los datos que identifican una comunicación. Sin embargo, la reforma aprobada por el Senado y pendiente de aprobación por la Cámara de Diputados se establece una excepción para la obtención de autorización judicial federal. En concreto la Minuta propone la siguiente adición al artículo 291:

> *"También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones privadas, así como la información, documentos, archivos de texto, audio, imagen o vídeo contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos vinculados a éstos, sin embargo, en el caso de que éstos se encuentren en el lugar de la posible comisión de un hecho delictivo y sin que exista persona detenida, el Ministerio Público podrá ordenar la extracción de información sin que medie la solicitud correspondiente a la autoridad judicial."*

La última porción del párrafo que se pretende adicionar al CNPP genera una excepción que no tiene justificación y que desnaturaliza el principio de autorización judicial previa. En este sentido, de aprobarse la adición al artículo 291 se vulneraría de manera clara los estándares constitucionales e internacionales que reconocen el principio de autorización judicial y por tanto no debe ser aprobada por la Cámara de Diputados.

Asimismo, para la vigilancia, el artículo 301 establece obligaciones de colaboración vagas e

ilimitadas a concesionarios, permisionarios y cualquier titular de medios o sistemas susceptibles de intervención:

> *Artículo 301. Colaboración con la autoridad*
>
> *Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con las disposiciones aplicables. Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas.*
>
> *El incumplimiento de este mandato será sancionado conforme a las disposiciones penales aplicables.*

Esta facultad es demasiado amplia y puede comprometer de manera grave la seguridad e integridad de comunicaciones y sistemas. Deben establecerse límites claros a los tipos de colaboración y, en todo caso, estos siempre deben ser ordenados por la autoridad judicial y no por el Ministerio Público.

El mencionado artículo 301 debe ser modificado para limitar las formas de colaboración. De esta manera, el desarrollo de capacidades de vigilancia o cualquier otra medida que pueda comprometer la seguridad e integridad de dispositivos y sistemas, no pueden constituir métodos legítimos de colaboración.

Igualmente, el artículo 303 permite al Ministerio Público ordenar la localización geográfica en tiempo real de equipos de comunicación móvil, sin la necesidad de autorización judicial y para cualquier tipo de delito. Además, puede solicitar, sin que medie autorización judicial, la conservación de datos contenidos en redes, sistemas o equipos de informática, hasta por 90 días en los casos de delitos relacionados o cometidos con medios informáticos.

Una reforma aprobada por el Senado, pero pendiente de aprobación por la Cámara de Diputados, establece la necesidad de autorización judicial previa para la localización geográfica en tiempo real de equipos de comunicación de manera general. Esta reforma también requiere autorización judicial inmediata con efectos retroactivos en casos en que esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con secuestro, extorsión o delincuencia organizada.

Si bien esto representa un avance que debería ser aprobado por la Cámara de Diputados, según los estándares fijados por la Suprema Corte de Justicia de la Nación, la utilización de

esta herramienta debe limitarse a la investigación de ciertos delitos de especial gravedad, los cuales deben señalarse de manera específica en la ley. Además de aprobar la minuta en esta porción del artículo 303, debe especificarse para qué delitos es posible utilizar esta medida de vigilancia.

Igualmente, la minuta del Senado limita los sujetos obligados a cumplir órdenes de conservación de datos a los concesionarios de telecomunicaciones y requeriría autorización judicial para que dichas órdenes fueran válidas. Por lo tanto, dicha porción debe aprobarse, aunque sería útil que quede explícito en la ley que las órdenes de conservación de datos deben ser específicas y no masivas e indiscriminadas.

IV.2 Vigilancia Estatal de las Comunicaciones para la Prevención del Delito y para la Protección de la Seguridad Nacional

La legislación que establece facultades de vigilancia para la prevención del delito o para la protección de la seguridad nacional, como la Ley de la Policía Federal o la Ley de Seguridad Nacional, así como la legislación especializada en materia de secuestro y delincuencia organizada, deben establecer de manera clara, precisa y detallada los casos y circunstancias en los que la Policía Federal o el Centro de Investigación y Seguridad Nacional (CISEN) pueden llevar a cabo medidas de vigilancia.

En concreto, dichas autoridades únicamente deberían estar facultadas para llevar a cabo medidas de vigilancia cuando la amenaza de comisión de un delito o la amenaza para la seguridad nacional esté basada en evidencia que demuestre su realidad, actualidad e inminencia. En este sentido, no deben autorizarse medidas de vigilancia que tengan como objeto una prevención general.

En el caso de la seguridad nacional, la ley debe establecer de manera acotada y precisa los casos que constituyen amenazas a la seguridad nacional, las cuales deben ser entendidas como aquellas que verdaderamente ponen en riesgo, de manera demostrable, la integridad territorial y la existencia del Estado. En este sentido, no es legítimo justificar la vigilancia de comunicaciones bajo el concepto de "recolección de inteligencia".

Las autoridades capaces de llevar a cabo medidas de vigilancia deben estar establecidas de manera explícita y taxativa. En concreto, en cumplimiento de los señalado por el artículo 16 de la Constitución, únicamente pueden llevar a cabo medidas de vigilancia, para fines distintos a los de procuración de justicia, las autoridades federales que designe la ley. Por lo tanto, las policías de las entidades federativas, salvo que operen bajo el mando del Ministerio Público, no deben poseer facultades de vigilancia autónomas. Igualmente, las fuerzas

armadas no deben estar facultadas, en tiempos de paz, para llevar a cabo medidas de vigilancia de comunicaciones.

IV.3 Eliminación de la Conservación Indiscriminada de Datos

La obligación de conservación indiscriminada y masiva de datos de usuarios de telecomunicaciones establecida en el artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión debe ser eliminada en tanto es violatoria del derecho a la privacidad, como ha sido reconocido, por ejemplo, por el Tribunal de Justicia de la Unión Europea.[43]

Las órdenes de conservación de datos deben ser, en su caso, específicas y estar basadas en indicios de participación en un hecho delictivo, además de estar precedidas de autorización judicial.

IV.4 Claridad de Métodos de Colaboración

Las normas que establecen obligaciones de colaboración para la vigilancia, como el artículo 300 del Código Nacional de Procedimientos Penales y el artículo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión deben establecer de manera clara y precisa los métodos de colaboración permitida, estar siempre mediados por autorización judicial y debe incorporarse el principio de integridad y seguridad de sistemas,[44] de manera que se encuentre expresamente prohibida exigir el desarrollo de capacidades de vigilancia que comprometan la integridad y seguridad de sistemas de comunicación.

Por ejemplo, la indetectabilidad y las amplias capacidades de recolección de datos que posee el software malicioso de espionaje ("malware"), comprometen de manera grave el derecho a la privacidad y a la libertad de expresión. Inclusive, el abuso de este tipo de vigilancia ha sido demostrado de manera inequívoca al revelarse que autoridades como el Gobierno del Estado de Puebla (que no posee facultades legales de vigilancia), han utilizado ese tipo de software para espiar a adversarios políticos.[45] Además, existen fuertes indicios de que periodistas también habrían sido objetivos de este tipo de vigilancia.

La utilización de software malicioso para llevar a cabo medidas de vigilancia estatal debe considerarse, en principio, desproporcionada, y por lo tanto debería estar prohibida por la ley de manera general. De forma excepcional, los jueces deben limitar su uso a casos en los que no exista otra medida menos lesiva a través de la cual pueda conseguirse el objetivo legítimo perseguido y existir una estricta y permanente supervisión judicial del uso de este tipo de técnicas de vigilancia altamente invasivas.

IV.5 Transparencia

El avance logrado en el artículo 70, fracción XLVII de la Ley General de Transparencia y Acceso a la Información Pública debe traducirse en una implementación efectiva, de manera que la información estadística respecto de las medidas de vigilancia se publique de manera periódica en las páginas de internet de las autoridades que llevan a cabo este tipo de actividades.

Igualmente, el Instituto Federal de Telecomunicaciones, debe cerciorarse de que las obligaciones de transparencia en cabeza de las empresas concesionarias de servicios de telecomunicaciones establecidas en los "Lineamientos de Colaboración en materia de Seguridad y Justicia" sean cumplidas sin demora.

Asimismo, deben establecerse mecanismos de transparencia respecto de la adquisición, compra, importación y exportación de equipos o sistemas de vigilancia.

IV.6 Derecho de Notificación

Debe incorporarse el derecho de notificación al usuario. En concreto, toda ley que faculte a una autoridad a llevar a cabo medidas de vigilancia masiva, o en su defecto, una ley creada para ese efecto, debe reconocer el derecho de las personas a ser notificadas del hecho de haber sido sujetos de vigilancia. La notificación solamente debe diferirse cuando el juez encargado de otorgar la autorización determine que la notificación pondría en riesgo la consecución del interés legítimo. En todo caso, la ley debe fijar plazos máximos para el diferimiento de la notificación.

La notificación debe comprender todo el material obtenido por la autoridad de manera que la persona afectada pueda conocer el contenido y alcance de la invasión de su privacidad y pueda, en consecuencia, ejercer su derecho de acceso a la justicia para remediar cualquier abuso.

IV.7 Supervisión Independiente

La ley debe establecer un mecanismo de supervisión de las medidas de vigilancia o, en su defecto, deben otorgarse facultades explícitas de supervisión de los programas y mecanismos de vigilancia al Instituto Nacional de Acceso a la Información Pública y Protección de Datos (INAI), de manera que dicha autoridad tenga la obligación de fiscalizar el uso de medidas de vigilancia. Para ello, deben otorgarse a dicho Instituto, todos los recursos materiales y humanos, así como los poderes para acceder a toda la información que sea relevante para llevar a cabo dicha labor.

El mecanismo de supervisión independiente debe publicar y difundir ampliamente los hallazgos llevados a cabo en cumplimiento de sus obligaciones de supervisión y debe estar facultado para imponer sanciones, o en su defecto, para iniciar los procedimientos sancionatorios por el abuso de las medidas de vigilancia.

IV.8 Protección de Denunciantes

La ley debe reconocer la inmunidad de las personas que, de buena fe, denuncien la violación de la ley, actos de corrupción o violaciones a derechos humanos en incumplimiento de un deber de secrecía. Esta inmunidad debe estar explícitamente reconocida en la legislación que impone sanciones penales o administrativas por el incumplimiento de estos deberes de secrecía.

IV.9 Recurso Efectivo

La Ley de Amparo debe ser interpretada por el Poder Judicial de la Federación de manera que se reconozca la legitimación procesal de cualquier persona para reclamar la inconstitucionalidad de normas que establecen medidas de vigilancia encubierta, sin que sea necesario probar la aplicación concreta de dicha norma a la persona que interpone una demanda de amparo.

Dada la naturaleza secreta de las medidas de vigilancia, resulta imposible para las personas detectar las invasiones a su privacidad ilegítimas y, por ende, combatirlas judicialmente si se exige prueba de un acto de aplicación.

Por lo tanto, en aras de respetar el derecho a un recurso efectivo, debe reconocerse el interés jurídico o legítimo de cualquier persona para desafiar judicialmente este tipo de normas, como por ejemplo, ya lo ha resuelto el Segundo Juzgado de Distrito Especializado en Telecomunicaciones en el juicio de amparo 116/2014.[46]

1 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text, EFF, ARTICLE19, Análisis Jurídico Internacional de Apoyo y Antecendentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal, Access, Guía de Implementación Universal de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf

2 Suprema Corte de Justicia de la Nación. Primera Sala. Amparo en Revisión 1621/2010 y Contradicción de Tesis 194/2012.

3 Suprema Corte de Justicia de la Nación. Primera Sala. Contradicción de Tesis 194/2012.

4 Suprema Corte de Justicia de la Nación. Segunda Sala. Amparo en Revisión 964/2015.

5 Suprema Corte de Justicia de la Nación. Primera Sala. Amparo en Revisión 1621/2010 y Contradicción de Tesis 194/2012.

6 Suprema Corte de Justicia de la Nación. Primera Sala. Amparo en Revisión 1621/2010.

7 Suprema Corte de Justicia de la Nación. Primera Sala. Amparo en Revisión 1621/2010 y Contradicción de Tesis 194/2012.

8 Suprema Corte de Justicia de la Nación. Segunda Sala. Amparo en Revisión 964/2015.

9 Suprema Corte de Justicia de la Nación. Pleno. Acción de Inconstitucionalidad 32/2012.

10 Suprema Corte de Justicia de la Nación. Pleno. Contradicción de Tesis 293/2011.

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

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

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

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

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

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

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

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

19 Análisis Jurídico Internacional de Apoyo y Antecedentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal

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

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

22 Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de Abril de 2013. A/HRC/23/40, disponible en inglés en: https://eff.org/r.z5x

23 Declaración Conjunta sobre Programas de Vigilancia y su Impacto para la Libertad de Expresión, disponible en: https://eff.org/r.maus

24 CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

25 Principios Globales sobre Seguridad Nacional y el Derecho a la Información ("Principios de Tshwane") concluidos en Tshwane, Sudáfrica y emitidos el 12 de junio de 2013, disponible en: https://eff.org/r.flb4

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

27 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.

28 Animal Político. México, el principal cliente de una empresa que vende software para espiar, disponible en: https://eff.org/r.4aob

29 Animal Político / R3D. SEDENA negoció compra de software de Hacking Team en 2015 para espiar a 600 personas, disponible en: http://www.animalpolitico.com/2015/07/sedena-negocio-compra-de-software-a-hacking-team-en-2015-para-espiar-a-600-personas/

30 Código Federal de Procedimientos Penales. Artículos 278 Bis y 278 Ter.

31 Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro. Artículos 24 y 25

32 Ley Federal contra la Delincuencia Organizada. Artículos 8 y 16 a 28.

33 Gaceta Parlamentaria de la Cámara de Diputados. 10 de Diciembre de 2014.

34 Ley de la Policía Federal. Artículos 48 a 55.

35 Ley Federal de Telecomunicaciones. Artículo 44 fracción XII y XIII.

36 Acuerdo/016/2014 por el que el Titular de la Unidad de Inteligencia Financiera designa a los servidores públicos que se mencionan en el presente para efectos de lo dispuesto en el artículo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión publicado en el Diario Oficial de la Federación el 15 de agosto de 2014.

37 Reuters. Mexico ramps up surveillance to fight crime, but controls lax. Disponible en: http://www.reuters.com/article/2015/10/12/us-mexico-surveillance-idUSKCN0S61WY20151012

38 Suprema Corte de Justicia de la Nación. Segunda Sala. Amparo en Revisión 964/2015.

39 Instituto Federal de Telecomunicaciones. Lineamientos de Colaboración en materia de Seguridad y Justicia. Publicados en el Diario Oficial de la Federación el 2 de Diciembre de 2015. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

40 Ley de Seguridad Nacional. Artículos 33 a 49.

41 Juzgado Segundo de Distrito en Materia Administrativa, Especializado en Competencia Económica, Radiodifusión y Telecomunicaciones, con residencia en el Distrito Federal y Jurisdicción en toda la República. Amparo Indirecto 116/2014 (Carlos Alberto Brito Ocampo y otros). Sentencia de 16 de Febrero de 2015.

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

43 TJUE. Sentencia en los asuntos acumulados C-293/12 y C-594/12. Digital Rights Ireland y Seitlinger y otros. 8 de abril de 2014, disponible en: https://eff.org/r.1f5l . Comunicado de Prensa. El Tribunal de Justicia declara inválida la Directiva sobre la conservación de datos, disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf

44 El Principio de Integridad de las Comunicaciones y Sistemas, indica que "a fin de garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que poner en peligro la seguridad con fines estatales casi siempre afecta la seguridad en términos generales, los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado. La retención o la recopilación de datos a priori nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anónimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios".

45 Animal Político / R3D. El Gobierno de Puebla utilizó el software de Hacking Team para espionaje político, disponible en: http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/

46 Juzgado Segundo de Distrito en Materia Administrativa, Especializado en Competencia Económica, Radiodifusión y Telecomunicaciones, con residencia en el Distrito Federal y Jurisdicción en toda la República. Amparo Indirecto 116/2014 (Carlos Alberto Brito Ocampo y otros). Sentencia de 16 de Febrero de 2015,disponible en: https://eff.org/r.ncyl