Comentarios al Anteproyecto de Dictamen del Código Nacional de Procedimientos Penales[1]

Resumen Ejecutivo

El anteproyecto de dictamen del Código Nacional de Procedimientos Penales (en adelante "el anteproyecto") contiene diversas disposiciones relativas a la intervención de comunicaciones privadas y otras interferencias con el derecho a la privacidad para la consecución del objetivo legítimo de la investigación y persecución de delitos.

El anteproyecto contiene algunos avances respecto del marco jurídico vigente, por ejemplo, el establecimiento de la obligación por parte de las procuradurías, de obtener autorización judicial federal para la intervención de comunicaciones privadas, incluyendo los datos que identifican una comunicación.

No obstante, el anteproyecto no establece salvaguardas suficientes para inhibir los riesgos de abuso de este tipo de medidas como lo es la notificación diferida, medidas de transparencia estadística, supervisión independiente e incluso, en el caso de la localización geográfica, en tiempo real, de equipos de comunicación móvil, no requiere autorización judicial. Por lo tanto se concluye que el anteproyecto no cumple con las obligaciones constitucionales y convencionales en materia de derechos humanos, en particular, el derecho a la privacidad.

Al respecto, esta opinión recomienda la modificación del anteproyecto a la luz de la jurisprudencia y doctrina constitucional e internacional en materia del derecho a la privacidad y tomando como guía a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

El derecho a la privacidad y a la inviolabilidad de las comunicaciones privadas

[1] Elaborado por Luis Fernando García Muñoz. Licenciado en Derecho por la Universidad Iberoamericana. Candidato a Maestro en Derecho Internacional de los Derechos Humanos por la Universidad de Lund, Suecia.

El derecho a la privacidad, y en particular, a la inviolabilidad de las comunicaciones privadas se encuentra reconocido en el artículo 16 constitucional, así como en el artículo 11 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos.

La Suprema Corte de Justicia de la Nación (en adelante "SCJN") ha tenido la oportunidad de desarrollar el contenido y alcance del artículo 16 constitucional en ocasiones recientes. De sus decisiones se desprende que las comunicaciones privadas objeto de protección constitucional no se circunscriben solamente a la correspondencia de carácter escrito, sino que también comprende las comunicaciones realizadas por cualquier medio o artificio técnico desarrollado a la luz de las nuevas tecnologías[2].

La SCJN ha precisado que lo que el derecho a la inviolabilidad de las comunicaciones prohíbe, es la "intercepción o el conocimiento antijurídico de una comunicación ajena"[3]. A su vez ha señalado que este derecho "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[4]. Por lo tanto "la violación de este derecho se consuma en el momento en que se escucha, se graba, se almacena, se lee o se registra" de manera antijurídica una comunicación[5].

Adicionalmente, la SCJN[6] y la Corte Interamericana de Derechos Humanos[7] han establecido que el derecho a la inviolabilidad de las comunicaciones privadas no solamente protege la comunicación en sí misma, sino que se extiende a los datos

---

[2] SCJN. Tesis: 1ª. CLVIII/2011, Novena Época, 1ª Sala, Semanario Judicial de la Federación y su Gaceta, Tomo XXXIV, Agosto de 2011, página 217. Rubro: DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. MEDIOS A TRAVÉS DE LOS CUALES SE REALIZA LA COMUNICACIÓN OBJETO DE PROTECCIÓN.

[3] SCJN. Tesis: 2ª. LXIII/2008, Novena Época, 1ª Sala, Semanario Judicial de la Federación y su Gaceta, Tomo XXXIV, Agosto de 2011, página 221. Rubro: DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SUS DIFERENCIAS CON EL DERECHO A LA INTIMIDAD.

[4] Id.

[5] Id.

[6] SCJN. 1ª Sala. Amparo Directo en Revisión 1621/2010; SCJN. 1ª Sala. Contradicción de Tesis 194/2012; "DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE IDENTIFICAN LA COMUNICACIÓN". Novena Época, Instancia: Primera Sala, 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

[7] Corte Interamericana de Derechos Humanos. *Caso Escher y otros Vs. Brasil*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200.

que identifican la comunicación, también conocidos como “datos de tráfico de comunicaciones”, entre los que se encuentran el registro de números marcados por un usuario de la red telefónica, la identidad de los comunicantes, la duración de la llamada telefónica, la identificación de una dirección de protocolo de internet (IP) o la localización geográfica de los comunicantes.

De esta forma, cualquier interferencia con el derecho a la privacidad, especialmente al derecho a la inviolabilidad de las comunicaciones privadas, requiere que la injerencia esté prevista en ley, persiga un fin legítimo y sea necesaria en una sociedad democrática[8]. En el caso de la injerencia estatal en las comunicaciones privadas, ha sido ampliamente reconocido que “la naturaleza secreta y confidencial de esta facultad depositada en el ejecutivo conlleva un evidente riesgo de arbitrariedad”[9], por lo que se hace indispensable la adopción de salvaguardas suficientes y adecuadas para inhibir su abuso.

Para el cumplimiento del deber señalado en el párrafo anterior, el Relator Especial de las Naciones Unidas para la promoción y protección del derecho a la libertad de expresión y opinión, Frank La Rue, ha llamado recientemente a los Estados a revisar la legislación nacional que regula la vigilancia de las comunicaciones de manera que se adecúe a los estándares internacionales[10] a través de medidas como: la supervisión judicial independiente; el establecimiento de medidas relativas al alcance, naturaleza, duración y circunstancias en las que pueden adoptarse de medidas de vigilancia; la notificación diferida a la persona afectada; el acceso a un recurso judicial adecuado y efectivo; el respeto al principio de proporcionalidad; la supervisión por un órgano independiente; medidas de transparencia y otras medidas que inhiban el abuso de las facultades de vigilancia.

Asimismo, como resultado de una consulta global con grupos de la sociedad civil, industria y expertos en legislación sobre vigilancia de las comunicaciones, políticas públicas y tecnología, han sido desarrollados los Principios Internacionales sobre

---

[8] Id.
[9] Tribunal Europeo de Derechos Humanos. Caso de Weber y Saravia c. Alemania. Sentencia de 29 de junio de 2006, párr. 93; Caso Kennedy c. Reino Unido. Sentencia de 18 de mayo de 2010, párr. 152; Caso Malone c. Reino Unido. Sentencia de 2 de agosto de 1984, párr. 67; y Caso Rotaru c. Rumania. Sentencia de 4 de mayo de 2000.
[10] ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. 17 de abril de 2013. A/HRC/23/40

la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones[11] (en adelante "los Principios"), los cuales constituyen una guía para la regulación de la vigilancia de las comunicaciones de manera compatible con las obligaciones de derechos humanos. De esta forma, para que las medidas previstas en el Anteproyecto puedan considerarse compatibles con las obligaciones en materia de derechos humanos, estas deben cumplir, entre otros, con los siguientes principios:

- **Legalidad:** Cualquier limitación al derecho a la privacidad debe estar contemplada en una ley, en el sentido formal y material, que indique de manera clara y precisa los supuestos para la interferencia.

- **Objetivo Legítimo:** La limitación debe perseguir un fin legítimo que corresponda a un interés jurídico preponderante y que sea necesario en una sociedad democrática.

- **Necesidad:** La vigilancia de las comunicaciones debe ser estrictamente necesaria para alcanzar el objetivo legítimo. Por lo tanto, la vigilancia sólo debe llevarse a cabo de manera excepcional, cuando no exista un medio menos restrictivo para la consecución del objetivo legítimo perseguido.

- **Proporcionalidad:** La vigilancia de las comunicaciones debe ser considerada como un acto altamente intrusivo que interfiere con los derechos a la privacidad y la libertad de opinión y de expresión, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la vigilancia de las comunicaciones deben tomarse sopesando el beneficio que se persigue contra el daño que se causaría a los derechos de las personas y contra otros intereses en conflicto, y debería incluir un examen de la sensibilidad de la información y de la gravedad de la infracción al derecho a la privacidad.

  En concreto, esto requiere que en el acceso o uso de información obtenida a través de vigilancia de las comunicaciones en el marco de una

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

investigación penal, debe establecerse ante una autoridad judicial competente, independiente e imparcial que:

1. Existe un alto grado de probabilidad de que un delito grave ha sido cometido o será cometido;
2. La evidencia sobre tal delito sería obtenida al acceder a la información protegida que se busca;
3. Otras técnicas de investigación que son menos invasivas y están disponibles ya han sido agotadas;
4. La información a la que se tiene acceso se limitará a la razonablemente relevante para el presunto delito y cualquier exceso en la información recopilada será destruido o devuelto sin demora, y
5. Solo tendrá acceso a la información la autoridad especificada y se utilizará solo para el propósito para el cual se le dio autorización.

- **Autorización Judicial:** Una autoridad judicial imparcial e independiente debe autorizar toda medida de vigilancia de las comunicaciones y supervisar de manera periódica el cumplimiento de las condiciones y alcances establecidos en la autorización.

- **Debido Proceso:** Debe garantizarse el debido proceso en la autorización de medidas de vigilancia. Por lo tanto debe establecerse, de manera detallada, el procedimiento legal para la autorización de medidas de vigilancia, el cual debe garantizar que toda persona afectada tenga acceso a un recurso para remediar cualquier violación a sus derechos. Sólo en casos de emergencia, donde exista un riesgo inminente de peligro para la vida humana, podrá dispensarse el cumplimiento de algunos requisitos. En tales casos, deberá buscarse una autorización con efecto retroactivo de manera expedita.

- **Notificación del Usuario:** Las personas afectadas por una medida de vigilancia deben ser notificadas sobre cualquier decisión que autorice la vigilancia de sus comunicaciones. La notificación debe incluir los materiales presentados en apoyo de la solicitud de la autorización, así como la

información personal que haya sido obtenida a través de la medida. La notificación debe ocurrir lo más pronto posible, el retraso en la notificación solo estaría justificada cuando:

1. La notificación podría en serio peligro la investigación o exista un riesgo inminente de peligro para la vida humana;
2. La autorización para retrasar la notificación es otorgada por la autoridad judicial que concedió la autorización de la vigilancia;
3. La persona afectada es notificada tan pronto como el riesgo desaparece o dentro de un periodo de tiempo razonable y factible.

- **Transparencia:** Debe garantizarse la transparencia sobre el uso y el alcance de las técnicas y los poderes de vigilancia de las comunicaciones. Debe publicarse de manera periódica, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, según el tipo de investigación y sus propósitos. Debe permitirse que los proveedores de servicios publiquen los procedimientos que adoptan y estadísticas sobre la colaboración con la autoridades para la vigilancia de las comunicaciones.

- **Supervisión Independiente y Pública:** Deben establecerse mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones. Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, cuando sea el caso, el acceso a información secreta o clasificada, para valorar si el Estado está haciendo un uso legítimo de sus funciones legales, para evaluar si el Estado ha sido transparente y ha publicado información precisa sobre el uso y el alcance de las técnicas y poderes de vigilancia de las comunicaciones; y para publicar periódicamente informes y otra información relevante para la vigilancia de las comunicaciones.

- **Integridad de las Comunicaciones y Sistemas:** No debe obligarse a proveedores de servicios a construir la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de vigilancia. La retención o la recopilación de datos a priori nunca debe ser exigida a los proveedores de servicios.

- **Garantías contra el Acceso Ilegítimo:** Debe penalizarse la vigilancia ilegal de las comunicaciones por agentes públicos o privados. Cualquier información obtenida de manera ilegal debe ser considerada inadmisible como prueba, al igual que cualquier evidencia derivada de dicha información, asimismo dicho material debería ser destruido o devuelto a la persona afectada.

Análisis del Anteproyecto de Código Nacional de Procedimientos Penales.

En los artículos 288 a 300 del Anteproyecto, se pretende regular la intervención de comunicaciones privadas como técnica para la investigación de delitos. Si bien, se establece un procedimiento y algunas medidas de supervisión y control, se considera que la regulación de esta facultad no cumple con los principios desarrollados anteriormente como a continuación se desarrolla.

La redacción del artículo 288 sugiere que basta con que la Procuraduría considere necesaria la intervención de comunicaciones privadas para que esta debe ser autorizada por la autoridad judicial federal. La necesidad y en concreto, la causa probable de comisión o participación en un hecho delictivo deben ser aspectos evaluados por la autoridad judicial de manera independiente a las consideraciones de la Procuraduría. Por lo tanto debe clarificarse el sentido de este artículo de manera que se garanticen los principios de necesidad y proporcionalidad.

En el artículo 300 se autoriza a las Procuradurías a solicitar, sin autorización judicial, la localización geográfica en tiempo real de los equipos de comunicación móvil asociados a una línea relacionados con cualquier investigación. Lo anterior incumple el principio de autorización judicial, generando incentivos para el abuso de esta medida. El monitoreo de la localización geográfica puede revelar

información altamente sensible sobre una persona, por lo tanto, no debe disminuirse la protección a estos datos. A su vez, resultaría contradictorio que el acceso a información conservada sobre la localización geográfica de los interlocutores de una comunicación requiera autorización judicial, como lo señala el artículo 288 y el acceso a la misma información en tiempo real no requiera dicha autorización judicial. Por lo tanto, resulta fundamental que se establezca el requisito de autorización judicial para la localización geográfica, en tiempo real de equipos de comunicación móvil.

A su vez, resulta preocupante que el artículo 300 abra la posibilidad para utilizar dicha herramienta para cualquier investigación, cuando la disposición vigente (cuya constitucionalidad está cuestionada en la Acción de Inconstitucionalidad 32/2012) limita su utilización para ciertos delitos de especial gravedad.

La parte final del artículo 300 también resulta preocupante, en tanto faculta a las Procuradurías a requerir a concesionarios, permisionarios o comercializadoras del servicio de telecomunicaciones la conservación de datos contenidos en redes, sistemas o equipos de informática. No es claro si los datos que se mencionan se refieren a datos de localización o si se refiere a cualquier dato que identifica una comunicación. En cualquier caso, la retención de datos, independientemente del acceso a los mismos, debe estar precedida de autorización judicial federal. Como lo ha señalado la SCJN y la Corte Interamericana, los datos que identifican la comunicación también se encuentran protegidos por el derecho a la inviolabilidad de las comunicaciones y el objeto de protección de ese derecho es tanto el conocimiento, como el almacenamiento, conservación o registro, es decir, la retención de datos, al constituir una interferencia en el derecho a la privacidad, debe cumplir los requisitos para la limitación del derecho a la privacidad. Por lo tanto debe modificarse el Anteproyecto, debe eliminarse la obligación de retención de datos de la Ley Federal de Telecomunicaciones y, en su caso, debe regularse el procedimiento de solicitud y autorización judicial para la retención de datos personales en posesión de particulares, especialmente los relacionados con las comunicaciones.

El Anteproyecto no contempla otras medidas necesarias para garantizar que la vigilancia de las comunicaciones no sea abusada. En particular, no se contempla

el derecho de notificación a la persona cuyas comunicaciones y datos personales son retenidos u obtenidos por la autoridad. Lo anterior resulta sumamente riesgoso pues, entre otras cosas, puede impedir el derecho de acceso a un recurso efectivo, especialmente en los casos en que la investigación se encuentra archivada o se decreta el no ejercicio de la acción penal. De esta forma, el Anteproyecto debe ser modificado de manera que se garantice el principio de notificación al usuario.

A su vez, no se contempla la supervisión independiente del sistema de vigilancia a través de un órgano como el Instituto Federal de Acceso a la Información y Protección de Datos u otro órgano de supervisión especializado, encargado de fiscalizar el sistema. Debe considerarse la posibilidad de que dicho ente participe en las audiencias de autorización de intervenciones, de manera que se otorgue equilibrio al proceso de autorización.

Tampoco se establecen obligaciones de transparencia estadística que permitan a los órganos supervisores, al poder legislativo y a la ciudadanía en general conocer el alcance y volumen de la utilización de medidas de vigilancia de las comunicaciones. Deben establecerse obligaciones en este sentido, de manera que periódicamente las Procuradurías, el Poder Judicial Federal y los proveedores de servicios que colaboren con la autoridad emitan informes de transparencia. Esta obligación no debe obstaculizarse por el deber de secrecía establecido en el artículo 299.

Finalmente, los artículos 290 y 298 establecen la obligación de concesionarios, permisionarios y demás titulares de medios o sistemas susceptibles de intervención de colaborar “eficientemente” con la autoridad, inclusive, requiriéndose a los particulares el contar con capacidades indispensables para atender las exigencias requeridas por la autoridad. Lo anterior, de no ser limitado, puede poner en riesgo la integridad y seguridad de equipos y sistemas. No debe permitirse que, a través de esta facultad, se requiera a proveedores de servicios de comunicación o de manufactura de hardware o software el incluir capacidades para la vigilancia que pongan en riesgo la privacidad y seguridad de los usuarios. Por lo tanto debe ser modificada esta facultad de manera que se limiten sus alcances.

Recomendaciones

A la luz del análisis realizado se concluye que el Dictamen del Código Nacional de Procedimientos Penales debe incluir modificaciones que lo hagan compatible con las obligaciones en materia de derechos humanos, en particular se recomienda:

1. Modificar el artículo 288 y 290 de manera que se garantice que la autoridad judicial federal sea la encargada de evaluar la necesidad y proporcionalidad de la medida en lo términos señalados en este documento.
2. Modificar el artículo 300 de manera que se establezca la obligación de obtener autorización judicial federal para la localización geográfica, en tiempo real, de equipos de comunicación móvil y establecer de manera clara los supuestos en que dicha medida podrá ser autorizada.
3. Deben eliminarse en el Anteproyecto y en la Ley Federal de Telecomunicaciones, las obligaciones de retención indiscriminada de datos. En su caso, debe regularse el procedimiento de solicitud y autorización judicial para ello, atendiendo a los principios de necesidad, proporcionalidad y debido proceso.
4. Debe establecerse el derecho de notificación a la persona afectada por la técnicas de vigilancia como la intervención de comunicaciones privadas y la localización en tiempo real.
5. Deben establecerse obligaciones de transparencia estadística periódica, con el desglose y detalle suficiente para conocer y evaluar el alcance, volumen y eficacia de las medidas de vigilancia de las comunicaciones.
6. Debe establecerse un mecanismo de supervisión independiente (se sugiere al Instituto Federal de Acceso a la Información y Protección de Datos), que evalúe de manera permanente la utilización de medidas de vigilancia de las comunicaciones.
7. Se eliminen o modifiquen los artículos 290 y 298, de manera que se garantice que los particulares no se vean obligados a facilitar la vigilancia de las comunicaciones a costa de la integridad y seguridad de las comunicaciones y los sistemas.