Código Procesal Penal Federal

#REFORMA ESPIA

Comentarios a la regulación de nuevas técnicas de vigilancia en el proyecto de reforma

Abril 2018

por los Derechos Civiles

Índice

#ReformaEspía: Nuevas técnicas de vigilancia para la investigación penal*

El Senado está considerando dar media sanción a un proyecto de ley que autoriza el uso de sofisticadas tecnologías de vigilancia para la investigación de delitos. El aspecto problemático de la iniciativa es que no contempla todas las garantías adecuadas para evitar un abuso de herramientas que en otros países han dado lugar a casos de espionaje invasivo y sistemático. De este modo, los derechos humanos de las personas pueden verse seriamente amenazados por este proyecto, si no se toman los recaudos necesarios para protegerlos.

A continuación, describiremos el recorrido seguido por la iniciativa en el Senado. Luego, explicaremos las disposiciones que contiene la iniciativa en materia de vigilancia electrónica y señalaremos cuáles son los principales inconvenientes que presenta desde el punto de vista de los derechos humanos. Finalmente, propondremos algunas sugerencias y recomendaciones para que el proyecto pueda verse enriquecido.

I. Historia del proyecto

El 11 de Abril la Comisión de Justicia y Asuntos Penales del Senado de la Nación emitió dictamen favorable al proyecto de reforma del Código Procesal Penal de la Nación, presentado por los senadores Rodolfo Urtubey y Pedro Guastavino (ambos del Partido Justicialista). El argumento para esta iniciativa es la necesidad de incorporar al Código instituciones que ya estaban vigentes en otras leyes sancionadas en los últimos tiempos (como la flagrancia o la figura del arrepentido, entre otras). Visto de esta manera, pareciera que la intención del proyecto es solamente ordenar en un cuerpo único lo que ya está previsto en la legislación actual.

Sin embargo, lo anterior no es totalmente correcto. La iniciativa busca, además, incorporar medidas que hoy no están vigentes en la República Argentina. Tal es el caso del capítulo de "Técnicas espe-

*El presente documento fue escrito por **Eduardo Ferreyra,** abogado y analista de políticas públicas, y **Leandro Ucciferri**, abogado e investigador, miembros del Área Digital de la Asociación por los Derechos Civiles (ADC). https://adcdigital.org.ar | https://adc.org.ar

ciales de investigación", en donde se consagran diversas medidas de vigilancia electrónica, acústica y de comunicaciones para la investigación criminal. Esta disposición refleja lo previsto en un proyecto de ley del 2016, que realizaba diversas modificaciones al Código Procesal Penal de la Nación. Pero a diferencia de otras medidas, las técnicas de vigilancia electrónica nunca fueron establecidas en alguna ley independiente posterior. Es por ello que en los fundamentos del proyecto, no se menciona expresamente la incorporación de medidas de vigilancia electrónica.

El tratamiento del proyecto por parte de la Comisión de Justicia y Asuntos Penales fue realizado de manera express, es decir, sin abrir la discusión a representantes de la sociedad civil, académicos o expertos del ámbito técnico. Si tenemos en cuenta que la iniciativa busca incorporar institutos no vigentes todavía en nuestro país, hubiera sido deseable que se habilitara la intervención de la mayor cantidad de puntos de vista, más si tenemos en cuenta la naturaleza sensible de las medidas a implementar. En este sentido, la Coalición por la Reforma Procesal Penal - integrada por organizaciones de la sociedad civil que incluyen a ACIJ, APP, INCEIP, CELS y ADC-, envió una carta al Senado para que abra el debate del proyecto, debido a –entre otras cosas– la incorporación de tecnologías de vigilancia, las cuales presentan desafíos para la protección de los derechos humanos –en particular, el derecho a la privacidad– y las garantías constitucionales.

El proyecto iba a ser tratado por el Senado el pasado miércoles 18 de abril pero finalmente los legisladores decidieron tratar otros temas. Las informaciones que circulan hasta este momento indican que el proyecto sería considerado en la sesión de este miércoles 25 de abril.

II. Análisis de las disposiciones del proyecto en materia de vigilancia electrónica

La regulación de las nuevas medidas de vigilancia está prevista en los capítulos I y II del Título VI titulado "Técnicas especiales de investigación". El capítulo I se encarga de establecer los lineamientos principales.

En primer lugar, se establece como norma general la obligación de observar los principios de necesidad, razonabilidad y proporcionalidad, al momento de aplicar las medidas de vigilancia. En segundo lugar, se prevé que toda medida de investigación deberá ser solicitada por un fiscal y autorizada por orden judicial. Para ello, el juez tendrá que haber:

1. Comprobado que la medida a adoptarse se encuentra relacionada con la investigación de un "delito concreto de especial gravedad";

2. Evaluado la verosimilitud de la sospecha de que alguien, como autor o partícipe, haya cometido, o intentado cometer, el delito objeto de la investigación;

3. Descartado que no existan otras medidas menos gravosas para el investigado que resulten igualmente útiles para el esclarecimiento de los hechos o para averiguar el paradero de los imputados;

4. Acreditado la existencia de una probabilidad suficientemente motivada de que una o varias de las medidas a adoptar proporcionarán elementos de prueba significativos para el avance de la investigación;

5. Ponderado que el beneficio para el interés público que espera obtenerse guarde adecuada relación de proporcionalidad con la afectación de los derechos e intereses involucrados.

Por último, el capítulo determina que la duración de la medida dependerá de lo que establezca la orden que la autorice, la cual podrá ser renovada si todavía existen las causas que le dieron orígen. Quizás para contrarrestar esta flexibilidad en el tiempo, la iniciativa contempla que luego de 1 año de otorgada la medida, un juez de revisión deberá controlar los motivos aducidos para su continuidad. Respecto a la medida de vigilancia remota sobre equipos informáticos, el proyecto sí establece una duración máxima de 1 mes. Sin embargo, dicha medida también puede ser prorrogada, si hay motivos fundados.

La iniciativa consagra adecuadamente la necesidad de respetar los principios de necesidad, razonabilidad y proporcionalidad, tal como es establecido por los estándares internacionales de derechos humanos. Sin embargo, al momento de concretizar dicha garantía en el resto de las disposiciones, el proyecto resulta defectuoso de dos maneras: ya sea por la inclusión de normas que -al contrario de los previsto por los principios- apuntan a un uso de las tecnologías de vigilancia más amplio de lo necesario, o por la omisión en incorporar reglas que limitarían la utilización de herramientas tan invasivas, como las que se pretende autorizar.

Comencemos por analizar los requisitos que el juez debe considerar para ordenar que se recurra a una medida de vigilancia de este tipo.

La iniciativa habla de que debe tratarse de un *"delito concreto de especial gravedad"*. La ambigüedad del concepto permite que su determinación quede sujeta al criterio del juez, lo cual implica que el campo de aplicación de las medidas será mayor o menor de acuerdo al parecer del magistrado interviniente. Esta falta de certeza entra en tensión con una interpretación razonable de los principios generales, que apuntan a limitar el catálogo de delitos que pueden ser investigados por estas tecnologías mediante una determinación previa y clara de los mismos. Este problema se intensifica en este caso ya que el proyecto no establece pautas para calificar un delito como de "especial gravedad". En este sentido, se debe remarcar que para otro tipo de medidas de igual sensibilidad –como el agente encubierto o el agente revelador– el proyecto sí ha establecido un listado concreto de delitos en los cuales puede recurrirse a ese tipo de medidas.

Luego, se establece que la sospecha debe ser verosímil. En este punto, el proyecto también falla en fijar límites eficaces, ya que le no exige ningún grado específico de sospecha para autorizar este tipo de medidas. En este sentido, la iniciativa se aleja de otras legislaciones más garantistas, las cuales especifican una escala de sospechas, según la gravedad de la injerencia y la importancia del derecho fundamental. Alemania, por ejemplo, distingue entre "sospecha inicial", "sospecha cualificada" y "sospecha suficiente o imperiosa", y sólo en este último caso autoriza la utilización de las medidas más severas. Por el contrario, según la letra del proyecto, cualquier leve sospecha –mientras sea verosímil– permite recurrir a una medida de vigilancia especial.

Asimismo, el carácter sensible de varias de las medidas implica que no es suficiente el que *"no existan otras medidas menos gravosas para el investigado que resulten igualmente útiles"*. Las medidas de vigilancia propuestas deberían siempre ser consideradas como *última ratio* en la investigación penal debido a su fuerte injerencia en la vida privada de las personas involucradas y potenciales terceros ajenos a la investigación. Es por ello que al igual que en el caso anterior, debería establecerse una distinción según la gravedad de los delitos y permitir las medidas más invasivas únicamente cuando otras alternativas sean notoriamente ineficaces o desproporcionadamente inútiles.

Por otro lado, la ausencia de una duración específica de las medidas de vigilancia (con la excepción ya señalada de la medida de acceso remoto) junto con la posibilidad de ser renovadas continuamente también resulta un obstáculo para el objetivo de atenuar al máximo posible el uso de estas herramientas. Sin un plazo expreso o un límite a la renovación, las personas pueden verse sujetas a una vigilancia indefinida de sus conversaciones, comunicaciones o movimientos. Si bien la iniciativa intenta establecer condiciones –que subsistan las causas que dieron origen a la medida, que se expongan los avances logrados o el control de un juez revisor–, no se prevé la intervención del investigado. De esta manera, el derecho de defensa se resiente, ya que no existe la posibilidad de que la persona pueda brindar argumentos para evitar que se continúe con la medida aplicada. Finalmente, tampoco se consagra una sanción expresa y específica para el fiscal que no cumpla con la obligación de cesar la vigilancia cuando no hay motivo para hacerla.

Luego de las normas generales, el capítulo II se dedica a enumerar las medidas de vigilancia adoptadas: vigilancia acústica, vigilancia de las comunicaciones, vigilancia remota sobre equipos informáticos y vigilancia a través de dispositivos de seguimiento y localización.

Cada una de estas medidas implica poner en manos del Estado la potestad de utilizar herramientas tecnológicas con capacidades altamente intrusivas de la intimidad de las personas.

Por ejemplo, la vigilancia acústica habilita al Estado a utilizar micrófonos para grabar conversaciones del investigado, siempre y cuando se encuentren fuera del domicilio de cualquiera de los interlocutores. Hoy en día es posible encontrar en el mercado micrófonos tan grandes como una tarjeta de crédito (llegando a un rango aproximado de 12 metros), o diminutos como el botón de una camisa. Los audios grabados luego pueden ser procesados con tecnologías de identificación biométrica,

específicamente reconocimiento de voz, para identificar inequívocamente al interlocutor.

Por otra parte, la vigilancia a través de dispositivos de seguimiento y localización habilita, por ejemplo, el uso de rastreadores equipados con GPS para conocer en tiempo real la ubicación geográfica del investigado, ya sea directamente de su persona o de un vehículo. Además, tecnologías como IMSI-Catchers (o *Stingrays*, por su nombre comercial), permiten simular una antena celular con el fin de captar las señales de los teléfonos en un radio determinado (aprox) para conocer con un mayor grado de precisión la ubicación del teléfono móvil del investigado.

A nivel global, la industria comercial del malware maneja miles de millones de dólares al año en transacciones. En los últimos años, la cantidad de empresas que ofrecen servicios profesionales de malware, orientados específicamente a fuerzas de seguridad y otros organismos Estatales, ha crecido exponencialmente. Desde el 2015, dos empresas han cobrado especial relevancia en América Latina, la italiana Hacking Team y la israelí NSO Group; con más firmas siendo creadas periódicamente.

Organizaciones de la sociedad civil como Citizen Lab, R3D y Derechos Digitales, han investigado y denunciado exhaustivamente el uso del malware comercializado por Hacking Team y NSO, fundamentalmente por parte de actores gubernamentales, siendo México el principal país comprador de este tipo de tecnología en la región.

El software comercializado por Hacking Team, Remote Control System, o Pegasus en el caso de NSO Group, permite –una vez infectado el dispositivo– acceder a todo tipo de información, desde contactos, fotos, ubicación geográfica por GPS, o el texto que se escribe en el teclado, hasta la posibilidad de prender los micrófonos, grabar las llamadas, u obtener capturas de pantalla, todo sin el conocimiento de la persona que utiliza el dispositivo.

La sensibilidad de las medidas a implementar debe tener como correlato el establecimiento de fuertes obligaciones en cabeza del Estado para evitar un abuso de las mismas. Sin embargo, el proyecto falla en fijar las garantías necesarias. Sin agotar la lista, podemos mencionar las siguientes omisiones:

- No existe una obligación de notificar al sujeto investigado de que está siendo objeto de una medida de vigilancia, en aquellos casos en que no hay razón para creer que la notificación resultará en un perjuicio para la investigación. Esta notificación es particularmente importante en el caso de acceso remoto a equipos informáticos y cuando la vigilancia se extiende por mucho tiempo.

- No establece una regulación expresa para el caso de que los datos se encuentren en un servidor ubicado en país extranjero. De esta manera, se deja abierta la posibilidad de que la investigación acceda a ellos, sin la intervención de las autoridades del Estado donde eventualmente están alojados.

- No existe un deber por parte de las autoridades de publicar reportes periódicos de transparencia

acerca del alcance de las operaciones de vigilancia llevadas a cabo (usuarios afectados, aparatos afectados, duración de las operaciones, etc).

- No está prevista la obligación de informar públicamente las tecnologías adquiridas o de permitir auditorías externas -u otro mecanismo de control similar- sobre ellas.

- No hay límites explícitos acerca del alcance de la información que puede ser recolectada, quiénes pueden acceder a ella, cuánto tiempo puede ser conservada o si puede ser transferida a otros órganos o para otros fines. Tampoco está prevista la intervención de la autoridad de protección de datos como instancia de autorización o control de la legalidad del procedimiento.

- No se establece la creación de un órgano independiente, transparente e imparcial para que lleve adelante la realización de estas actividades tan intrusivas.

Dos casos en particular merecen una atención separada, debido a su especial sensibilidad.

El primero de ellos es la **afectación a personas que no forman parte de la investigación**. Como hemos dicho anteriormente, la característica altamente invasiva de las medidas de vigilancia puede llevar a que la intimidad de terceros pueda verse afectada por una investigación en la cual no están involucradas. De esta forma, el uso de determinadas tecnologías de vigilancia que, debido a su accionar en un rango operativo establecido, pueden captar información en forma indiscriminada sobre terceros no contemplados en la investigación; por ejemplo, tal es el caso de IMSI-Catchers y micrófonos.

El proyecto sostiene que ,de todos modos, dichas medidas podrán ser llevadas a cabo cuando el efecto sea "*inevitable*". Más allá de la total ausencia de pautas para determinar cuándo esos efectos serán inevitables –lo que entra en tensión nuevamente con los principios de necesidad o razonabilidad–, la iniciativa no establece ningún recaudo o medida para el manejo de la información recolectada sobre terceros. En particular, no hay prevista ninguna obligación de notificación al tercero o de destrucción de los datos adquiridos. Esto resulta particularmente grave ya que –repetimos– se trata de información sensible sobre personas que no están siendo investigadas.

El segundo de ellos es la **autorización para utilizar vigilancia remota sobre equipos informáticos**. Esta técnica de investigación contempla el uso de software para acceder en forma subrepticia –es decir, sin conocimiento de la persona investigada y terceros ajenos a la investigación– a dispositivos electrónicos, como computadoras, smartphones y tablets, sistemas informáticos, bases de datos o instrumentos de almacenamiento masivo de datos informáticos. De esta manera, el proyecto está legalizando actividades de hackeo estatal contra particulares.

De acuerdo a su redacción actual, el proyecto omite considerar cuestiones esenciales para un ejercicio legítimo de dicha facultad. ¿Quién sería el responsable de llevar adelante dichas actividades? ¿Cuál sería el software utilizado? ¿El software sería comprado como una solución empaquetada a empresas

especializadas o desarrollado por el mismo Estado? ¿Se llevarían a cabo auditorías –idealmente independientes– para asegurarse que el software hace exclusivamente lo que se determinó en la orden autorizada por el juez? ¿Qué tipo de mecanismos de control se pondrían en lugar para una adecuada rendición de cuentas del uso del software y las operaciones llevadas a cabo con el mismo?

Debido a la acotada descripción prevista por la disposición del proyecto, no queda claro qué tipo de software será utilizado específicamente, ni cómo se pondrá en práctica. Por ejemplo, un escenario posible sería el uso de algún tipo de malware –un programa o archivo que tiene como objetivo manipular o ejecutar determinadas funciones en el dispositivo de su objetivo, generalmente sin su conocimiento ni consentimiento– para ingresar a la computadora o smartphone de la persona bajo investigación y así obtener información que luego será utilizada como prueba.

III. Sugerencias para mejorar el proyecto

A partir de las consideraciones realizadas, sugerimos los siguientes aportes para mejorar la protección de las personas al momento de llevar a cabo una medida especial de vigilancia.

1. Establecer un listado concreto de delitos en los cuales se podrá recurrir a este tipo de medidas para su investigación. Debido al carácter sensible de las herramientas tecnológicas, el recurrir a este tipo de medidas debería ser la excepción y por ende, su procedencia debe ser limitada a supuestos expresamente previstos con anticipación.

2. Determinar una clasificación de la intensidad de la sospecha de la persona investigada y en base a dicha distinción, permitir el uso de las tecnologías más invasivas únicamente cuando exista un sospecha suficiente o imperiosa.

3. Consagrar un robusto principio de subsidiariedad y en consecuencia, autorizar el uso de las herramientas más sensibles sólo cuando las otras alternativas de investigación hayan demostrado ser notoriamente inútiles o ineficaces para lograr el éxito de la investigación.

4. Fijar un límite temporal cierto, tanto para la duración de las medidas de vigilancia como para la cantidad de veces que puede ser renovada. En todos las casos, debería darse participación al investigado para que pueda ofrecer sus argumentos acerca de la procedencia o no de la medida.

5. Disponer la obligación de notificar a la persona de que está siendo objeto de investigación, sobre todo en aquellos casos en los que la comunicación no supone un peligro para la eficacia de pesquisa. En caso que la hubiere, deberá disponerse la notificación dentro de un plazo razonable posterior a su realización.

6. Distinguir los casos en que la información se encuentra alojada en un servidor ubicado en el extranjero. En este caso, el procedimiento para poder acceder a estos datos debería ser como regla general el establecido en los Tratados de Asistencia Legal Mutua o en mecanismos de cooperación internacional similar. De esta manera, el Estado en donde están alojados los datos podrá colaborar en controlar la legalidad del procedimiento.

7. Establecer la obligación de publicar periódicamente informes de transparencia con los detalles de las operaciones de vigilancia llevadas a cabo. De este modo, la sociedad tendrá la oportunidad de controlar la efectividad y legitimidad de las actividades producidas.

8. Permitir la realización de auditorías externas e independientes de las tecnologías que se usarán para las medidas de vigilancia. Así, las personas investigadas podrán tener una mayor seguridad en la confiabilidad e integridad de las herramientas utilizadas y habrá una instancia de control imparcial encargada de velar porque la obtención de la información sea efectuada de manera legítima.

9. Instaurar un marco regulatorio de la adquisición, acceso, manejo, transmisión y eliminación de los datos obtenidos. Para ello, debería convocarse a la autoridad de protección de datos personales del país para que participe en el proceso de autorización, elaboración y control de las operaciones de vigilancia que se lleven a cabo.

10. Crear un órgano independiente, transparente e imparcial encargado de llevar adelante o supervisar las operaciones de vigilancia que sean autorizadas.

11. Extremar las precauciones respecto a la información obtenida de personas que no forman parte de la investigación, en particular la obligación de notificar al tercero y de destruir de inmediato los datos obtenidos.

12. Considerar como regla general la prohibición por parte del Estado de realizar actividades de hackeo sobre particulares y permitir este tipo de medidas únicamente como último recurso, en casos excepcionales, dentro de un período de tiempo claramente establecido y cuidando de no violar la intimidad y demás derechos humanos.

13. Deben establecerse disposiciones específicas que prohíban hacer uso de vulnerabilidades en software o hardware de dispositivos electrónicos utilizados masivamente en el mercado doméstico, puesto que ello representa poner en riesgo la seguridad digital colectiva. Teniendo como posible efecto adverso la pérdida de confianza de la ciudadanía en el uso de tecnologías cotidianas, desde Internet hasta sus smartphones o computadoras.