El nuevo régimen de las medidas intrusivas tecnológicas y de las "técnicas especiales de investigación" en la Ley Nº 21.577, de 15 de julio de 2023

Héctor Hernández Basualto
Universidad Diego Portales

El siguiente corresponde a un informe analítico elaborado a petición de la Defensoría Penal Pública sobre la Ley Nº 21.577, de 15 de junio de 2023, en lo concerniente a las medidas intrusivas tecnológicas y a las llamadas "técnicas especiales de investigación" que regula, sobre todo desde la perspectiva de los presupuestos de legitimidad de su aplicación y sus posibles consecuencias en términos de admisibilidad probatoria.

I. La situación previa a la Ley Nº 21.577 y los alcances sistemáticos de esta

Cualquier observador del régimen legal de las medidas intrusivas tecnológicas y de las "técnicas especiales de investigación" en Chile, (entrega vigilada, agentes encubiertos, agentes reveladores e informantes) aprecia inmediatamente un escenario de dispersión. La Ley Nº 21.577, de 15 de junio de 2023, tiende a superar ese escenario, pero, como se verá, solo parcialmente.

El texto original del Código Procesal Penal[1] de 2000 contenía, además de las medidas intrusivas tradicionales (entrada y registro de lugares cerrados, exámenes corporales, retención e incautación de correspondencia), la de interceptación de comunicaciones telefónicas (arts. 222 a 225)[2], y otra denominada genéricamente "otros medios técnicos de investigación" (art. 226), en tanto

[1] En lo sucesivo, artículos sin otra mención corresponden a los de este código.

[2] Antes del Código Procesal Penal de 2000, solo la Ley Nº 18.314, de 17 de mayo de 1984, sobre conductas terroristas, consideraba la posibilidad de interceptar comunicaciones en el contexto de un proceso penal sobre esos delitos, entendiéndose que incluía la interceptación de las comunicaciones telefónicas (así, por ejemplo, *Bofill*, Jorge: Las prohibiciones de prueba en el proceso penal, Revista de Derecho de la Universidad Católica de Valparaíso, XII [1988], 225 [240, 242]), en un art. 14 al que, luego del retorno a la democracia, se le agregó una referencia explícita al respecto, pero como medida específica a disponer respecto del procesado preso (Ley Nº 19.027, de 24 de enero de 1991), agregado que, sin embargo, en el contexto de la reforma procesal penal (Ley Nº 19.806, de 31 de mayo de 2002), fue el único que subsistió, con lo cual las interceptaciones dejaron de ser posibles respecto de simples delitos terroristas,

que no preveía ninguna regulación sobre entrega vigilada, agentes encubiertos, agentes reveladores o informantes, instituciones que solo se consideraban rudimentariamente en la Ley Nº 19.366, de 30 de enero de 1995, sobre tráfico ilícito de estupefacientes y sustancias sicotrópicas, en los arts. 29 (entrega vigilada) y 34 (agentes encubiertos e informantes, de un modo oblicuo, a propósito de la denegación del conocimiento del sumario en razón de su seguridad)[3].

En razón de que las mencionadas *medidas intrusivas tecnológicas* solo podían disponerse en la investigación de hechos constitutivos de crimen, se fueron incorporando, tanto en el Código Penal (en lo sucesivo, CP) como en leyes especiales, disposiciones que las hacían excepcionalmente aplicables en la investigación de ciertos simples delitos. Tal es el caso, en el código punitivo, de los delitos asociados a la pornografía y a la prostitución infantil, conforme al inciso primero del art. 369 ter CP, introducido por la Ley Nº 19.927, de 14 de enero de 2004; de aquellos de tráfico ilícito de migrantes y de trata de personas, de acuerdo con el inciso segundo del art. 411 octies CP, introducido por la Ley Nº 20.507, de 8 de abril de 2011; y de hurto o robo de madera (sobre cierto valor), en virtud del inciso segundo del art. 448 septies CP, introducido mediante la Ley Nº 21.488, de 27 de septiembre de 2022 (por remisión al antiguo art. 226 bis)[4]. En el Código Procesal Penal, por el viejo art. 226 bis, sobre

no obstante que algunos de los delitos previstos por la ley, aun con el aumento de pena propio de la ley, son simples delitos.

[3] Debe mencionarse también que la Ley Nº 19.974, de 2 de octubre de 2004, sobre sistema de inteligencia del Estado, prevé en su art. 24, como "procedimientos especiales de obtención de información", la intervención de comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas, la intervención de sistemas y redes informáticos, la escucha y grabación electrónica, incluyendo la audiovisual, y la intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información, con autorización de un Ministro de Corte de Apelaciones (art. 25); asimismo, se prevé el empleo de agentes encubiertos e informantes, sin necesidad de autorización judicial (arts. 31 y 32). El uso de estas herramientas debe limitarse "a actividades de inteligencia y contrainteligencia que tengan por objetivo resguardar la seguridad nacional y proteger a Chile y su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico" (art. 23). Satisfechos sus estándares de legitimidad, los resultados de estos procedimientos pueden eventualmente ser usados como prueba en el proceso penal, como se desprende del art. 39.

[4] El precepto del Código Penal se remite a las "técnicas especiales de investigación" del art. 226 bis, lo que, considerando que esta expresión suele emplearse para referirse a la entrega vigilada y a la intervención de agentes encubiertos y similares, podría entenderse que se trata de una remisión limitada a esos supuestos, no a las medidas intrusivas tecnológicas, pero, en la medida en que el epígrafe del art. 226 bis (dado por la propia ley) hablaba indistintamente de "técnicas especiales de investigación" y las trataba en conjunto, no parecía haber mucho espacio para tal lectura restrictiva.

el que se volverá luego, los de la Ley de Control de Armas, el art. 190 de la Ley del Tránsito y ciertos simples delitos contra la propiedad. En lo que respecta a leyes especiales, la Ley Nº 20.000, de 16 de febrero de 2005, que reemplazó la Ley Nº 19.366 en materia de drogas, en su art. 24 hizo aplicables (nombrándolas, no identificándolas formalmente) las medidas intrusivas tecnológicas, de conformidad con el Código Procesal Penal, a la investigación de los delitos previstos en la ley, "cualquiera sea la pena que merecieren", lo que rige también para la investigación de los delitos de lavado de dinero (no obstante ser crímenes y, por ello, no necesitarlo), en virtud de lo dispuesto en el art. 33 de la Ley Nº 19.913, de 18 de diciembre de 2003, que se remite para estos efectos a la Ley Nº 20.000; y más recientemente, el inciso primero del art. 12 de la Ley Nº 21.549, de 20 de junio de 2022, que hace aplicables los arts. 222 a 226 a la investigación de la mayoría de los delitos informáticos previstos en la misma ley.

En cuanto a la *entrega vigilada y a la actuación de agentes encubiertos, agentes reveladores e informantes*, fue la ya mencionada Ley Nº 20.000, sobre tráfico de drogas, la que introdujo un estatuto más completo de estas instituciones, en sus arts. 23 y 25, al que se remiten, expresa o tácitamente, otras disposiciones para hacerlas aplicables en la investigación de otros delitos. Es el caso de los delitos de lavado de dinero (entrega vigilada, agentes encubiertos e informantes), conforme al art. 33 de la Ley Nº 19.913; delitos informáticos (agentes encubiertos), de acuerdo con el inciso tercero del art. 12 de la Ley Nº 21.459; por el viejo art. 226 bis, los crímenes contra la propiedad (agentes encubiertos e informantes) y de la Ley de Control de Armas (agentes reveladores); relacionados con la pornografía y prostitución infantil (entrega vigilada y agentes encubiertos), conforme al inciso segundo a cuarto del art. 369 ter CP; de tráfico ilícito de migrantes y trata de personas (agentes encubiertos e informantes), de acuerdo con el inciso primero del art. 411 octies CP; de abigeato (entrega vigilada), de acuerdo con el inciso cuarto del art. 448 quáter CP; y, a través de una remisión al art. 226 bis, el robo y hurto de madera, conforme al inciso segundo del art. 448 septies CP. Como una peculiaridad de la regulación, puede adelantarse desde ya que el empleo de estas técnicas está o ha estado sometido a la exigencia de *autorización judicial* previa solo en algunos casos (los de los arts. 369 ter, 411 octies y 448 septies CP, del art. 12 de la Ley Nº 21.459 y del antiguo art. 226 bis), pudiendo el Ministerio Público disponerlas directamente en los demás.

Ante este panorama de dispersión, un primer intento, si bien modesto, de sistematizar la materia antes de la Ley Nº 21.577, lo constituyó la introducción del ya mencionado art. 226 bis ("técnicas especiales de investigación") mediante la Ley Nº 20.391, de 5 de julio de 2016, que hizo aplicables, por una parte, las medidas previstas en los arts. 222 a 226 en la investigación de un grupo de simples delitos, distintos de los ya considerados mediante disposiciones espe-

ciales: los de la Ley de Control de Armas, el art. 190 de la Ley del Tránsito, robos con fuerza, el hurto agravado del art. 447 bis, abigeato y receptación; y, por la otra, la aplicación de entregas vigiladas y el uso de agentes encubiertos e informantes (con autorización judicial) en la investigación de los crímenes de robo con violencia o intimidación, piratería y robo con fuerza en las cosas en lugar habitado o destinado a la habitación o en sus dependencias, así como el empleo de agentes reveladores respecto de la investigación de los delitos de la Ley de Control de Armas, todo de acuerdo con los arts. 23 y 25 de la Ley Nº 20.000. Presupuesto de aplicación de estas medidas y técnicas, además de que fuera indispensable o necesaria, era que:

> "existieren fundadas sospechas, basadas en hechos determinados, de la participación en una asociación ilícita, o en una agrupación u organización conformada por dos o más personas, destinada a cometer los hechos punibles previstos en estas normas, aun cuando ésta o aquella no configure una asociación ilícita".

El art. 226 bis fue modificado, primero, mediante la Ley Nº 21.412, de 25 de enero de 2022, sobre armas, eliminándose todas las referencias a los delitos de la Ley de Control de Armas, en consonancia con la introducción en dicha ley de un nuevo art. 19 B, que hacía aplicables las técnicas especiales del Título II de la Ley Nº 20.000 a la investigación de los delitos contenidos en ella, y, segundo, por la Ley Nº 21.488, de 27 de septiembre de 2022, sobre robo y hurto de madera, que agregó este delito, tipificado en el art. 448 septies CP, en el listado de los simples delitos cuya investigación admite el uso de las medidas de los arts. 222 a 226. Fue suprimido, por último, por la Ley Nº 21.577, que nos convoca.

No puede hablarse de una sistematización lograda, en la medida en que, al mismo tiempo, no se eliminaron las reglas especiales dispersas, con lo cual, más bien, se adicionaron nuevos regímenes. Así, respecto de las medidas intrusivas tecnológicas, estas pasaron a proceder en tres grupos de casos: cuando se investigaba un crimen, cuando se investigaba un simple delito de los señalados en el art. 226 bis y se daba el factor organizativo y, por último, cuando se investigaba un simple delito respecto del cual había norma especial expresa que lo hacía procedente. Y respecto de las entregas vigiladas, agentes encubiertos, agentes reveladores e informantes, el art. 226 bis agregó, a los casos previstos en normas especiales, un conjunto acotado de delitos en cuya investigación pasaron a ser aplicables estas técnicas, a condición de que se diera el factor organizativo.

En ese sentido, la Ley Nº 21.577, que, entre otras cosas, suprime el art. 226 bis, representa un avance en términos de sistematización, aunque tampoco se puede decir que bien logrado. El art. 226 A, a pesar de su defectuosa ubicación sistemática, a la cabeza del apartado I sobre "medidas intrusivas

referidas a las comunicaciones, imágenes y sonidos, y al registro de equipos informáticos", es, en realidad, la regla que define el ámbito de aplicación de todo el nuevo Párrafo 3º bis del Título I del Libro II, dedicado a las "[d]iligencias especiales de investigación aplicables para casos de criminalidad organizada" ("de este Párrafo", dice el precepto). Y lo hace en los siguientes términos:

> "Las técnicas especiales de investigación previstas en este Párrafo serán aplicables en la investigación de hechos que involucren la participación en una asociación delictiva o criminal, de acuerdo con lo previsto en los artículos siguientes" (inciso primero).

Tales técnicas especiales son, por una parte, las medidas intrusivas tecnológicas y, por la otra, la entrega vigilada y la acción de agentes encubiertos, agentes reveladores e informantes.

Es respecto de las segundas que el efecto de ampliación y sistematización de la ley es más notorio y logrado, pues, hasta ahora, estas solo procedían respecto de la investigación de delitos puntual y taxativamente mencionados en normas especiales (lo que hacía el art. 226 bis era, simplemente, ampliar el catálogo de la mano del factor organizativo), mientras que ahora, además de los casos que siguen previstos en normas especiales, son aplicables en la investigación de cualquier delito, con tal que se dé el factor organizativo previsto por la ley. Lo que se echa en falta es que no se hubieran suprimido los casos especiales o que ni siquiera se hubieran modificado de acuerdo con el factor organizativo que parece justificar su uso, al menos respecto de la técnica más delicada, que es la actuación de agentes encubiertos (las entregas vigiladas y la acción de agentes reveladores o informantes pueden justificarse más fácilmente). Más aún, las modificaciones a los arts. 369 ter y 411 octies CP, que, si bien mencionaban la posible actuación de una organización, no la exigían, se limitan a eliminar esas referencias, enfatizando así la procedencia respecto de la investigación de actividad delictiva exclusivamente individual, sin que la remisión en lo demás al nuevo Párrafo 3º bis del Título I del Libro II del Código Procesal Penal, altere esta conclusión, porque se entiende que se trata de la regulación de ejecución, no de la procedencia de las técnicas en cuestión. Lo mismo rige respecto del art. 448 quáter, donde la remisión al nuevo estatuto en materia de entrega vigilada es manifiestamente para los efectos de la ejecución, no de su procedencia.

Respecto de las primeras (en realidad solo de las previstas en el art. 222 y 226, como se desprenden del modo en que están descritas, considerando, además, que el nuevo registro remoto del art. 225 bis es aplicable a la investigación de cualquier delito, *infra* II 3), el único efecto del art. 226 A es que las hace aplicables en la investigación de cualquier delito (no solo de crímenes), a

condición de que se dé el mencionado factor organizativo (inciso tercero)[5]. De no darse ese factor y no tratarse de la investigación de un crimen, las medidas intrusivas tecnológicas solo serán aplicables en virtud de alguna norma especial, si la hubiere (art. 24 de la Ley Nº 20.000, arts. 269 ter y 411 octies CP), ninguna de las cuales fue modificada a este respecto. Por su parte, la declaración de la procedencia de aplicar el art. 218 a la investigación de delitos con este factor organizativo (inciso segundo)[6], no tiene sentido, porque el art. 218 no tiene restricciones de aplicación. El precepto concluye con una remisión, en lo demás, al art. 222 (inciso cuarto). Pero, como se verá, la Ley Nº 21.577 incide también en el régimen general de las medidas intrusivas tecnológicas, es decir, con efectos para todos los casos en que son procedentes, aunque no esté involucrada una organización delictiva o criminal (*infra* II 1 a 4).

Se podría ver una modificación del régimen de investigación del hurto o robo de madera, del art. 448 septies CP, en la medida en que no fue modificado y, al mismo tiempo, se suprimió el art. 226 bis, al que aquel se remitía. Sin embargo, en la medida en que, como se vio, el art. 226 bis exigía factor organizativo, los casos en que procedían las medidas intrusivas tecnológicas y las "técnicas especiales de investigación" eran tendencialmente los mismos en que ahora proceden bajo el nuevo estatuto. Lo mismo puede decirse, y por la misma razón, de la investigación de los crímenes o simples delitos a que hacía referencia el viejo art. 226 bis, ahora suprimido.

Por último, una cuestión central en la aplicación del estatuto especial del nuevo Párrafo 3º bis será la comprobación, en todos los casos en que es el único presupuesto de procedencia de una medida o técnica, del factor organizativo previsto por la ley, a saber, que los hechos en cuestión "involucren la participación en una asociación delictiva o criminal".

No debiera haber muchas dudas respecto de que por "asociación delictiva o criminal" debe entenderse "toda organización formada por tres o más personas, con acción sostenida en el tiempo, que tenga entre sus fines la perpetración" de crímenes o simples delitos, como se desprende de los respectivos incisos terceros de los arts. 292 y 293 CP, introducidos por la misma ley. Nótese que se trata de una exigencia mayor que la prevista antes por el art. 226 bis, que

[5] "Las medidas de interceptación y grabación de comunicaciones, de conversaciones o imágenes obtenidos en lugares cerrados o que no sean de libre acceso al público serán aplicables, previa autorización judicial, cuando existan fundadas sospechas, basadas en hechos determinados, de la intervención en una asociación delictiva o criminal y su uso sea imprescindible para el éxito de la investigación".

[6] "Las medidas de retención e incautación de correspondencia y de obtención de copias de comunicaciones o transmisiones serán aplicables a la investigación según lo dispuesto en el artículo 218".

hacía bastar la participación en una agrupación u organización conformada por *dos* o más personas, destinada a cometer los hechos punibles del catálogo, "aun cuando ésta o aquella no configure una asociación ilícita".

Por otra parte, tampoco debiera haber dudas, al menos conceptuales, respecto de que, si en definitiva no se comprueba la participación de una asociación de estas características, los antecedentes obtenidos gracias a medidas o técnicas que solo eran procedentes en virtud de ese presupuesto, no pueden ser aprovechados como prueba. No necesariamente porque se hayan obtenido ilícitamente o con inobservancia de garantías fundamentales, juicio para el cual puede ser decisiva una perspectiva *ex ante*, sino simplemente por una consideración de proporcionalidad: no puede servir como prueba de un delito aquello que se obtiene con un medio cuyo empleo simplemente estaba vedado a la investigación de ese delito, por mucho que *prima facie* hubiera parecido procedente.

La pregunta central es, entonces, qué se va a exigir para entender, en definitiva, que se estaba frente a hechos que involucraban la participación en una asociación delictiva o criminal y que justificaban, en consecuencia, la aplicación de las medidas o técnicas en cuestión. La exigencia de una condena firme resulta excesiva, porque son muchas las razones por las cuales puede ser que el procedimiento, a ese respecto, legítimamente no llegue a término, a pesar de haber material probatorio que demuestra la existencia de una asociación de ese tipo. Por otra parte, los antecedentes (necesariamente preliminares, aún precarios) invocados durante la investigación para solicitar la autorización para el empleo de las medidas o técnicas no pueden ser fundamento suficiente. Pues es imperativo evitar que la mera invocación de la existencia de una asociación delictiva o criminal se convierta en un subterfugio suficiente para investigar siempre y en todo caso con medios extraordinarios, eludiendo abiertamente los límites impuestos por la ley para ello. Es tarea de los jueces evitarlo. De los jueces de garantía, en la audiencia de preparación de juicio oral; y del tribunal de juicio oral o simplificado, a la hora de valorar la prueba por delitos cuya investigación, se sabe ahora, no admitía el uso de las medidas o técnicas y la autorización para usarlas se basó en la circunstancia no comprobada.

En mi opinión, deben hacerse valer antecedentes suficientes como para tener por acreditada la "tipicidad objetiva" de los tipos penales de los arts. 292 o 293, esto es, la existencia de una asociación delictiva o criminal en los términos de esas disposiciones, así como una conexión entre la actividad de tal asociación y los hechos investigados. En cuanto no se trata de una decisión de condena, no debiera ser aplicable el estándar de convicción más allá de duda razonable, pero sí una convicción basada en antecedentes robustos. De no ser eso posible, no debería poder aprovecharse la prueba en cuestión, simplemente porque se obtuvo de un modo que estaba vedado, aunque a primera vista pudiera haberse visto de un modo diferente.

II. Análisis particular de las medidas intrusivas tecnológicas, con especial referencia a los presupuestos de legalidad y legitimidad

1. Interceptación y/o grabación de las telecomunicaciones de personas

Disposiciones aplicables:

I. Interceptación de comunicaciones

Art. 222. *Ámbito de aplicación.* El juez de garantía, a petición del Ministerio Público, podrá ordenar la interceptación y grabación de las comunicaciones telefónicas o de otras formas de comunicación cuando existan fundadas sospechas basadas en hechos determinados de que una persona ha cometido o participado en la preparación o comisión, o que ella prepara actualmente la comisión o participación en un delito al que la ley le asigna pena de crimen, y la investigación de tales delitos lo haga imprescindible.

La orden a que se refiere el inciso precedente sólo podrá afectar al imputado o a personas respecto de las cuales existieren fundadas sospechas basadas en hechos determinados, de que sirven de intermediarias de dichas comunicaciones y, asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios y la investigación de tales delitos lo hiciere imprescindible.

No se podrán interceptar las comunicaciones entre el imputado y su abogado, a menos que el juez de garantía lo ordenare, por estimar fundadamente, sobre la base de hechos determinados de los que dejará constancia en la respectiva resolución, que el abogado pudiere tener responsabilidad penal en los hechos investigados.

La orden que disponga la interceptación y grabación deberá consignar las circunstancias necesarias para individualizar o determinar al afectado por la medida y, de ser posible, los datos que permitan singularizar los medios de comunicación o telecomunicación a intervenir y grabar, tales como números de líneas telefónicas, direcciones IP, casillas de correos, entre otros. También señalará la autoridad o funcionario policial que se encargará de la diligencia de interceptación y grabación, la forma de la interceptación, su alcance y su duración.

La interceptación no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por períodos de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

Las empresas concesionarias de servicios públicos de telecomunicaciones y prestadores de servicios de internet deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado y bajo las medidas de seguridad correspondientes, a disposición del Mi-

nisterio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y prestadores de servicios deberán destruir en forma segura dicha información. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento.

Si las sospechas tenidas en consideración para ordenar la medida se disiparen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente.

Art. 223. *Registro de la interceptación.* La interceptación de que trata el artículo precedente será registrada mediante su grabación magnetofónica u otros medios técnicos análogos que aseguraren la fidelidad del registro. La grabación será entregada directamente al ministerio público, quien la conservará bajo sello y cuidará que la misma no sea conocida por terceras personas.

Cuando lo estimare conveniente, el ministerio público podrá disponer la transcripción escrita de la grabación, por un funcionario que actuará, en tal caso, como ministro de fe acerca de la fidelidad de aquélla. Sin perjuicio de ello, el ministerio público deberá conservar los originales de la grabación, en la forma prevista en el inciso precedente.

La incorporación al juicio oral de los resultados obtenidos de la medida de interceptación se realizará de la manera que determinare el tribunal, en la oportunidad procesal respectiva. En todo caso, podrán ser citados como testigos los encargados de practicar la diligencia.

Las comunicaciones que resulten impertinentes o irrelevantes para la investigación de los hechos de que se trate serán entregadas, en su oportunidad, a las personas afectadas con la medida. El Ministerio Público destruirá toda transcripción o copia de ellas.

Lo prescrito en el inciso precedente no regirá respecto de aquellas grabaciones que contengan informaciones relevantes para otros procedimientos seguidos por hechos que puedan constituir un delito al que la ley le asigne pena de crimen, de las cuales se podrá hacer uso conforme a las normas precedentes.

Art. 224. *Notificación al afectado por la interceptación.* La medida de interceptación será notificada al afectado por la misma con posterioridad a su realización, en cuanto el objeto de la investigación lo permitiere, y en la medida que ello no pusiere en peligro la vida o la integridad corporal de terceras personas. En lo demás regirá lo previsto en el artículo 182.

Art. 225. *Prohibición de utilización.* Los resultados de la medida de interceptación telefónica o de otras formas de telecomunicaciones no podrán ser utilizados como medios de prueba en el procedimiento, cuando ella hubiere tenido lugar

fuera de los supuestos previstos por la ley o cuando no se hubieren cumplido los requisitos previstos en el artículo 222 para la procedencia de la misma.

La Ley Nº 21.577 introdujo varias modificaciones a los arts. 222 y 223, ninguna de las cuales, sin embargo, parece especialmente trascendente. En varios casos se trata de simples cambios de redacción que no parecen incidir en el alcance de las normas. Puede aprobarse, por ejemplo, que, como fórmula para indicar en la investigación en qué delitos es procedente la medida intrusiva, se haya reemplazado la expresión delito o hecho punible "que merezca pena de crimen" por la más precisa de delito "al que la ley le asigne pena de crimen", aunque no se aprecia que la formulación inicial haya provocado grandes dudas respecto de que lo decisivo era la pena abstracta y no la concreta, sin contar con que el cambio no fue del todo consistente, pues la misma ley introduce en otras disposiciones la fórmula reemplazada (véase, por ejemplo, arts. 218 ter y 226 L inciso segundo).

La única mejoría apreciable, y relativamente menor, consiste en hacerse cargo abiertamente del problema práctico que representa la ausencia de datos exactos sobre el afectado y el medio a interceptar[7]. Así, mientras el inciso cuarto original disponía que la orden debía "indicar circunstanciadamente el nombre y dirección del afectado por la medida", la nueva redacción se refiere, más realistamente y en línea con el art. 24 de la Ley Nº 20.000, a que debe "consignar las circunstancias necesarias para individualizar o determinar al afectado por la medida", agregando que, de ser posible, debiera consignar "los datos que permitan singularizar los medios de comunicación o telecomunicación a intervenir y grabar, tales como números de líneas telefónicas, direcciones IP, casillas de correos, entre otros", así como "la autoridad o funcionario policial que se encargará de la diligencia de interceptación y grabación, la forma de la interceptación, su alcance y su duración". Esto es, por cierto, importante, pero, sin duda, no dará paso a una práctica mayormente diferente de la actual.

En rigor, lo único que en realidad llama la atención (para mal) del reciente proceso legislativo en relación con el art. 222 es una omisión que resulta del todo incomprensible, como es haber dejado incrustado en el inciso sexto una suerte de regulación parcial sobre *datos de tráfico*, en circunstancias en que la ley, precisamente, se hizo cargo del asunto, de modo completo y diferenciado, en el nuevo art. 218 ter (que se agrega al nuevo art. 218 bis, introducido mediante la Ley Nº 21.459, de 20 de junio de 2022, y que entra en vigor el 21

[7] El asunto lo hizo presente el Fiscal Nacional del Ministerio Público durante la tramitación legislativa, Informe de la Comisión de Seguridad Ciudadana de la Cámara de Diputados, de 5 de mayo de 2021, Biblioteca del Congreso Nacional: Historia de la Ley Nº 21.577 (HL Nº 21.577), p. 46 s.

de junio de 2024). En la medida en que ambas regulaciones se superponen al menos parcialmente, además de los defectos del art. 218 ter, son de prever dudas interpretativas significativas. El asunto se abordará con detalle *infra* 4, a propósito de la nueva regulación sobre la materia.

De ahí que el comentario de fondo sobre la interceptación de comunicaciones no verse, en rigor, sobre una innovación legislativa, sino que sobre un aspecto general de la regulación, tal como se introdujo por el Código Procesal Penal en 2000.

El punto que se quiere discutir aquí es el alcance del concepto de *comunicación* sometido al régimen del art. 222. En mi opinión, lo que regula el precepto es el acceso a (o la captación y grabación de) comunicaciones privadas *en tiempo real*, esto es, mientras estas están teniendo lugar, a lo que podría objetarse que dicha distinción, al menos a primera vista, no tendría sustento en la letra de la ley. Pero una distinción entre distintas formas de comunicación viene impuesta, como se verá, por la propia ley, y todo indica que el criterio que subyace a la distinción implícita en la regulación legal es, precisamente, si el acceso indebido a las comunicaciones privadas tiene lugar en tiempo real o no. En efecto, también la correspondencia epistolar, convencional o "en papel", es una "forma de comunicación privada" cuya inviolabilidad está garantizada por el art. 19 Nº 5 de la Constitución Política, pero es evidente, sin embargo, que los requisitos legales para acceder a ella (art. 218) no son los mismos, más específicamente, que son menos exigentes que los que rigen para poder escuchar una conversación telefónica (art. 222), desde luego, porque la retención de esa correspondencia procede respecto de la investigación de cualquier delito. Pero lo decisivo para el punto que aquí interesa, es que el criterio de distinción legal no gira en torno al empleo de medios tecnológicos para que se verifique la comunicación, como se desprende inequívocamente del hecho de que el mismo art. 218 que rige para los envíos postales convencionales y que no fue modificado por la Ley Nº 21.577[8], constituye la norma de cobertura para obte-

[8] "Art. 218. *Retención e incautación de correspondencia.* A petición del fiscal, el juez podrá autorizar, por resolución fundada, la retención de la correspondencia postal, telegráfica o de otra clase y los envíos dirigidos al imputado o remitidos por él, aun bajo nombre supuesto, o de aquéllos de los cuales, por razón de especiales circunstancias, se presumiere que emanan de él o de los que él pudiere ser el destinatario, cuando por motivos fundados fuere previsible su utilidad para la investigación. Del mismo modo, se podrá disponer la obtención de copias o respaldos de la correspondencia electrónica dirigida al imputado o emanada de éste. // El fiscal deberá examinar la correspondencia o los envíos retenidos y conservará aquellos que tuvieren relación con el hecho objeto de la investigación. Para los efectos de su conservación se aplicará lo dispuesto en el artículo 188. La correspondencia o los envíos que no tuvieren relación con el hecho investigado serán devueltos o, en su caso, entregados a su destinatario, a algún miembro de su familia o a su mandatario o representante legal. La correspondencia

ner "copias o respaldos de la *correspondencia electrónica* dirigida al imputado o emanada de éste" (inciso primero, *in fine*)[9]. Y si se pregunta ahora cuál es la diferencia que media entre acceder al correo electrónico y a las comunicaciones telefónicas de una persona, en términos de intensidad de la intromisión en la esfera de intimidad del sujeto, parece evidente que esta radica en ese carácter actual, simultáneo, "en tiempo real" de las segundas.

Otra manera de verlo, coincidente en el fondo, pero levemente diferente en la formulación, es distinguir entre comunicaciones que podrían calificarse de *efímeras*, de cuyo contenido[10], por las características mismas del medio empleado, no queda registro alguno, de aquellas otras en que necesariamente su contenido queda registrado. Desde cualquiera de las dos perspectivas, se entiende que existe una diferencia relevante en términos de afectación de derechos entre el acceso al correo electrónico y una conversación telefónica, que es lo que explica que las medidas intrusivas consistentes en el acceso a una u otra forma de comunicación estén sometidas a un régimen de legitimación también diferente.

Este criterio coincide con lo resuelto en su momento por jurisdicciones extranjeras enfrentadas al tratamiento del acceso al correo electrónico de una persona. Así, por ejemplo, en Alemania, a propósito de un caso en el que se había solicitado y concedido autorización judicial para acceder a correos electrónicos de un imputado, el Tribunal Supremo Federal resolvió que la medida estaba sujeta al régimen de legitimación de las incautaciones, particularmente de correspondencia convencional (§§ 94 y 99 StPO), y no al más exigente de la interceptación telefónica (§ 100a StPO). Lo interesante del pronunciamiento del BGH es que afirmó que la solución era la misma, fuera que los mensajes dirigidos al imputado hubieran sido ya leídos o no. Aunque el tribunal reconoce que el exacto *status* de los mensajes aún no leídos (en mi opinión, parece más razonable atender simplemente a si fueron ya "abiertos"), era dudoso a la época de la decisión, lo cierto es que no podía equipararse al de una comunicación telefónica, "porque durante el almacenamiento en el banco de datos del proveedor del servicio de correo electrónico (aunque

que hubiere sido obtenida de servicios de comunicaciones será devuelta a ellos después de sellada, otorgando, en caso necesario, el certificado correspondiente".

[9] La única disonancia que se puede advertir es que el inciso cuarto del art. 222 reformulado mediante la Ley Nº 21.577, dispone que la orden debe incluir, de ser posible, los datos que permitan singularizar los medios de comunicación a intervenir y grabar, y entre ellos menciona las "casillas de correos".

[10] Es difícil (si no imposible) que no quede ningún registro, siquiera brevemente, del hecho mismo de la comunicación. Es lo que pasa, por ejemplo, con los datos de tráfico telefónico.

posiblemente solo por una fracción de segundo), ya no hay un proceso de telecomunicación", de modo que la incautación de los correos ahí almacenados hasta una primera vista o vistas posteriores era plenamente comparable con la incautación de otros mensajes que quedan transitoriamente en poder de quien presta el servicio (sentencia de 31 de marzo de 2009, BGH NJW [*Neue Juristische Wochenschrift*] 2009, 1828).

Entre nosotros, este claro paralelismo con la correspondencia convencional explica que los correos electrónicos estén expresamente considerados en el art. 218, también desde un punto de vista de *proporcionalidad*. Pues no se aprecia absolutamente ninguna razón para que se puedan interceptar (en el sentido exacto de impedir que lleguen a destino) o retener sobres con cartas o incautar los mismos sobres antes o después de haberse enviado, como cualquier otro objeto, así como que se puedan incautar computadores y revisar todo lo que contienen, a propósito de la investigación de cualquier delito, y no se pudieran revisar, en cambio, los correos electrónicos almacenados en un computador incautado, sea de propiedad del emisor o receptor de los mensajes, sea de propiedad del prestador del servicio de correo. Lo mismo debiera regir, en consecuencia, para cualquier otra forma de comunicación que pase por el envío de mensajes que quedan almacenados, aunque sea por poco tiempo, para que el destinatario los pueda revisar en un momento posterior, tales como mensajes de texto (SMS) o mensajes de WhatsApp (también de audio).

Un aspecto dudoso, que marca, además, la diferencia entre los dos criterios de distinción presentados en principio como coincidentes (intromisión en tiempo real vs. intromisión diferida / registro o almacenamiento del mensaje vs. mensaje efímero, sin registro), surge al considerar aquellos casos en que se accede en tiempo real a una comunicación que tiene lugar a través de mensajes que quedan registrados, como sería el acceso a un intercambio por correo electrónico o por cualquier forma de chat mientras este está teniendo lugar. Según el primer criterio, se trataría de una interceptación en los términos del art. 222, según el segundo, no. Reconociendo que se trata de una cuestión muy discutible, aquí se está por el primer criterio, cuando menos considerando que la simultaneidad aumenta considerablemente la intensidad de la intromisión. Como es obvio, la disyuntiva solo se dará en la práctica cuando se pueda acceder remota y subrepticiamente a alguno de los equipos involucrados, de ahí que no extrañe que, en cuanto permite esa intromisión en tiempo real, en el derecho comparado se condicione dicha forma de acceso al cumplimiento de requisitos tanto o más exigentes que los que rigen para la interceptación, con independencia del tipo de comunicación efectiva o potencialmente afectada (sobre esto, *infra* 3).

2. Captación, grabación y registro subrepticio de imágenes o sonidos en lugares cerrados o que no sean de libre acceso al público

Normativa aplicable

> Art. 226. *Otros medios técnicos de investigación.* Cuando el procedimiento tenga por objeto la investigación de un hecho punible al que la ley asigna pena de crimen, el juez de garantía podrá ordenar, a petición del Ministerio Público, el empleo de medios tecnológicos para captar, grabar y registrar subrepticiamente imágenes o sonidos en lugares cerrados o que no sean de libre acceso al público, cuando existan fundadas sospechas basadas en hechos determinados y graves que lo hagan imprescindible para el esclarecimiento de los hechos. Regirán, en lo pertinente, las disposiciones de los artículos 222 a 225.

Al margen de defectos subsistentes, debe celebrarse, por cierto, la reformulación del art. 226, probablemente una de las disposiciones más defectuosas del código original. Tomada al pie de la letra, la formulación original del art. 226[11] conducía a resultados sencillamente absurdos. En efecto, al no precisar el contexto o las circunstancias específicas de las conductas que eran su objeto ("la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos"), se tendría que haber entendido, por ejemplo, que la fijación fotográfica de las marcas de frenado de un vehículo sobre la calzada por parte de la SIAT de Carabineros en el contexto de la investigación de un cuasidelito de homicidio o lesiones, asociado a un accidente de tránsito, no solo requería autorización judicial (aunque, ciertamente, no se lograra apreciar en ello la vulneración de las garantías fundamentales de nadie), sino que, además, por tratarse en ambos casos de la investigación de un simple delito, dicha autorización no hubiera sido procedente, pues la ley solo la permitía para la investigación de crímenes.

Como era obvio, no podía ser ese su sentido, que habría sido incongruente tanto con el art. 9º, que erige en presupuesto de la intervención judicial la afectación de derechos fundamentales, como con la amplísima definición de las actuaciones de investigación del art. 181, que, luego de mandar que se haga constar el estado de las personas, cosas o lugares, y se identifique e interrogue a los testigos, tomando nota de las huellas, rastros o señales que hubiere dejado el hecho, y dejando constancia de la descripción del lugar, del estado de los

[11] "Cuando el procedimiento tuviere por objeto la investigación de un hecho punible que mereciere pena de crimen, el juez de garantía podrá ordenar, a petición del ministerio público, la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos. Asimismo, podrá disponer la grabación de comunicaciones entre personas presentes. Regirán correspondientemente las normas contenidas en los artículos 222 al 225.".

objetos que en él se encontraren y de todo otro dato pertinente, afirma que "se podrá disponer la práctica de operaciones científicas, la toma de fotografías, filmación o grabación y, en general, la reproducción de imágenes, voces o sonidos por los medios técnicos que resultaren más adecuados", como, eventualmente, incluso, con la definición de las actuaciones autónomas de las policías, conforme al art. 83 letra c) o al art. 90. Con todo, era la letra de la ley.

La nueva redacción recoge, al menos en lo fundamental, lo que cualquier aproximación razonable al precepto adivinaba era su verdadero propósito y alcance, a saber, referirse a intromisiones tecnológicas *subrepticias y en tiempo real*, como se desprendía tanto del contexto sistemático, dominado por las interceptaciones telefónicas y similares, como de la referencia expresa a "la grabación de comunicaciones entre personas presentes", que solo tenía sentido práctico si la grabación era subrepticia, a la vez que representaba una intromisión de intensidad equivalente a la de una interceptación, lo que justificaba un régimen de garantía de tal intensidad. En efecto, ahora la ley se refiere al

> "empleo de medios tecnológicos para captar, grabar y registrar subrepticiamente imágenes o sonidos en lugares cerrados o que no sean de libre acceso al público".

Se trata, al menos, sin duda, de la captación, grabación o registro de imágenes o sonidos a los cuales un sujeto que no ha sido admitido a percibirlos por sus propios sentidos no podría acceder sin el empleo del medio tecnológico en cuestión. Es el caso de lo que ocurre al interior de un recinto cerrado bajo circunstancias concretas que impiden que alguien desde afuera pueda percibirlo de modo natural[12]. Se trata, por cierto, de micrófonos y/o cámaras dispuestas subrepticiamente al interior del recinto, pero también de medios tecnológicos que permitan ver o escuchar desde afuera, a pesar de los obstáculos a la percepción natural.

Lo mismo debiera regir, en principio, cuando los obstáculos no son permanentes o absolutos sino situacionales y lo que hace el medio tecnológico es, precisamente, suprimir el factor situacional. Así, por ejemplo, si se trata de

[12] En mi opinión, no están cubiertos los casos en que se puede ver y escuchar desde afuera, por falta de obstáculos para la visión humana (muros, puertas, cortinas, persianas, etc.) o el oído humano (un volumen que no permita que el sonido sea perceptible o inteligible por seres humanos que se encuentran fuera). El que gusta de los ventanales amplios o abomina de las cortinas, escucha música o programas de cualquier tipo a todo volumen o emite ruidos que simplemente se pueden escuchar desde afuera, porque son muy intensos o porque no se toma ningún resguardo para que otros no escuchen, como cerrar la ventana, no puede pretender que el mundo exterior no lo perciba. Por cierto, se puede discutir la legitimidad de grabar o registrar aquello que se puede percibir naturalmente, pero esa discusión no es distinta en casos como estos a la que puede darse sobre la captación o registro de lo que ocurre en la vía pública. En particular, no es una discusión que deba incidir en los alcances del art. 226.

una casa ubicada en un sector aislado, sin personas cerca, se puede asumir razonablemente que nadie podrá ver ni escuchar lo que pasa en el interior, aunque no haya cortinas ni persianas o se hable a los gritos, y por eso no se adoptan mayores resguardos, permitiendo inconscientemente que se capten, graben o registren imágenes y conversaciones privadas que no se hubieran sostenido en las mismas condiciones de haberse sabido que alguien las estaba captando a la distancia con dispositivos tecnológicos. O cuando es de noche y no hay luces ni adentro ni afuera que permitan que el ojo humano vea naturalmente el interior a pesar de la ausencia de cortinas o persianas y, sin embargo, se puede ver todo gracias a medios de visión nocturna o térmica. La validez de esta aproximación está condicionada, sin embargo, por el grado de generalización o masificación del uso de tales medios que el propio ordenamiento jurídico permite o al menos tolera. En un contexto social en el que los dispositivos de visión térmica o nocturna se convierten en un aparato ordinario de la vida cotidiana, que se puede adquirir en cualquier parte sin mayores restricciones, la pretensión jurídica de que la oscuridad brinde por sí sola protección contra la percepción ajena deja de ser plausible. Y algo similar puede decirse del uso de telescopios de todo tipo, o el uso de drones con cámaras y/o micrófonos.

A pesar del mérito general de la nueva formulación, la letra de la ley contiene dos exigencias que restringen innecesariamente la protección que debería brindar, ninguna de las cuales estaba presente en la redacción original, que, como se dijo, era defectuosa, pero por otras razones. La primera es que, al exigirse el "empleo de medios tecnológicos", no quedan cubiertos los casos en que una persona pueda captar subrepticiamente las imágenes o sonidos, por ejemplo, escondida dentro del recinto cerrado. Por supuesto esto requeriría autorización judicial, desde ya de acuerdo con el art. 205, pero no parece razonable que la instalación de un micrófono esté sometida a requisitos formales rígidos de proporcionalidad y a un régimen de control especial, y se pudiera, en cambio, esconder a un agente al interior de una morada para la investigación de cualquier delito y sin exigencias adicionales a la autorización judicial[13]. Si este ejemplo puede parecer de laboratorio, no lo son aquellos que produce la segunda exigencia legal que merece crítica, como es que lo captado, grabado o registrado

[13] Al margen de la disposición concreta que un juez pudiera tener ante una solicitud de este tipo (por ejemplo, aplicando un criterio equivalente al que aplica ante solicitudes en virtud del art. 222 o 226), se plantea la cuestión más fundamental sobre si el art. 9º es un mecanismo para validar progresivamente medidas intrusivas no previstas por la ley y que vayan surgiendo en la práctica (tesis con la cual, al menos *prima facie*, se está de acuerdo aquí) o si, por el contrario, al menos tratándose de intromisiones especialmente intensas, debe exigirse "reserva de ley", de modo que, en ausencia de previsión legal, la medida simplemente no es procedente.

debe tener lugar "en lugares cerrados o que no sean de libre acceso al público"[14], con lo cual no quedan cubiertos casos en los que, pese a no darse esa condición, resulta indudable una legítima expectativa de exclusión del acceso de otros. Con las imágenes ya se ha dicho que el asunto es cada vez más discutible, pero no parece serlo todavía respecto de los sonidos, por ejemplo, una conversación privada en voz baja o moderada en una playa desierta y que puede ser captada a distancia por un potente micrófono direccional. De nuevo, al menos debiera ser claro, todavía, que esa actividad requiere autorización judicial de acuerdo con las reglas generales, y en ese contexto el tribunal debiera aplicar criterios de proporcionalidad equivalentes a los de los arts. 222 o 226.

Que esta exigencia espacial se basa en una defectuosa comprensión de lo que debe ser protegido se confirma cuando no se considera solo su falla por defecto, sino también por exceso, concretamente cuando se considera la protección inusitada que se le da a lo que ocurre en lugares "que no sean de libre acceso al público", como podría ser un sitio cercado de propiedad privada, al que se puede ver desde edificios circundantes ¿requerirá autorización judicial filmar o fotografiar algo que se encuentre o pase ahí, y solo respecto de la investigación de crímenes, para que ese material audiovisual pueda aprovecharse en un proceso? La exigencia de actuar "subrepticiamente" debiera bastar para descartarlo en lo que concierne a las imágenes, de modo que no son de esperar graves consecuencias, pero se trata, sin duda, de una formulación defectuosa.

3. Registro remoto de equipos informáticos

Normativa aplicable

Artículo 225 bis. *Registro remoto de equipos informáticos y ámbito de aplicación.* A petición fundada del Ministerio Público, el juez de garantía podrá autorizar la utilización de programas computacionales que permitan acceder de manera remota y aprehender el contenido de un dispositivo, computador o sistema informático, sin conocimiento de su usuario, cuando existan fundadas sospechas basadas en hechos determinados, de que una persona ha cometido o participado en la preparación o comisión, o que el delito se esté cometiendo actualmente, o que se esté preparando la comisión o participación en una asociación delictiva o criminal.

La medida será autorizada por un plazo máximo de 30 días. El juez de garantía podrá prorrogar este plazo por períodos de hasta igual duración, con un máximo

[14] Es la misma restricción injustificada, en materia sustantiva, del tipo penal del art. 161-A CP.

de 60 días, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el inciso anterior.

Artículo 225 ter. *Requisitos de la resolución que autoriza la medida*. La resolución judicial que autorice el acceso remoto deberá especificar, a solicitud del fiscal:

a) Los dispositivos, computadores o sistemas informáticos específicos objeto de la medida y las circunstancias necesarias para individualizar o determinar al afectado por la medida.

b) El alcance de la medida, la forma en la que se procederá al acceso y aprehensión de contenidos relevantes para la causa y el programa computacional software mediante el cual se realizará acceso remoto.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los contenidos para la causa.

e) Las medidas técnicas específicas necesarias para preservar la integridad de los contenidos, así como para impedir el acceso y la supresión de dichos datos del sistema informático objeto de la medida.

f) La duración precisa de la medida.

Artículo 225 quáter. *Ampliación del registro*. Cuando al ejecutarse el acceso remoto surjan motivos para creer que los contenidos buscados están almacenados en otro sistema informático o en una parte de él, el juez de garantía, a petición fundada del Ministerio Público, podrá autorizar la ampliación de los términos del acceso remoto.

La resolución judicial que autorice la ampliación del registro deberá especificar los antecedentes señalados en el artículo anterior, que resulten pertinentes para el desarrollo de la ampliación.

Artículo 225 quinquies. *Deber de colaboración*. Los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información y los titulares o responsables del sistema informático o contenido objeto del acceso remoto, están obligados a colaborar con los funcionarios policiales encargados de ejecutar la medida. Asimismo, están obligados a facilitar la asistencia necesaria para que los contenidos aprehendidos puedan ser objeto de examen y visualización.

Los sujetos requeridos para prestar la colaboración en este tipo de requerimientos deberán guardar secreto acerca de los mismos, salvo que se les cite a declarar. La ejecución de la técnica de investigación, en los términos de la resolución judicial que la autoriza, no podrá ser objeto de sanción penal o civil.

Posiblemente la mayor innovación que trae consigo la Ley Nº 21.577 en materia de medidas intrusivas sea la introducción *ex nihilo* del registro remoto de equipos informáticos, en los arts. 225 bis a 225 quinquies. La medida consiste en "la utilización de programas computacionales que permitan acceder

de manera remota y aprehender el contenido de un dispositivo, computador o sistema informático" y esto "sin conocimiento de su usuario".

Se trata de una medida conocida en el derecho comparado, sometida, en general, a restricciones importantes, por la intensidad del efecto intrusivo que en concreto puede tener. Así, por ejemplo, en el derecho alemán (§ 100b StPO) solo procede para la investigación de delitos especialmente graves, especificados en un listado taxativo, mientras que en el derecho español (art. 588 septies a LECr), en general más laxo en estas materias, aunque los identifica de un modo más amplio, lo permite también solo para la investigación de ciertos delitos (cometidos en el seno de organizaciones criminales, de terrorismo, cometidos contra menores o personas "con capacidad modificada judicialmente", contra la Constitución, de traición y relativos a la defensa nacional, o bien cometidos a través de instrumentos informáticos o tecnologías de información o comunicación). Pero lo realmente significativo es que, en ambos ordenamientos, el registro remoto está sometido a exigencias *mayores* que las que rigen para las interceptaciones telefónicas (disponible, en Alemania, para la investigación de delitos contenidos también en un catálogo, pero considerablemente más amplio, § 100a II StPO; en España para la investigación de cualquier delito doloso castigado con pena máxima de tres años o más de prisión, además de delitos de terrorismo o cometidos en el seno de un grupo u organización criminal, art. 588 ter a en relación con art. 579.1 LECr). Esto contrasta significativamente con el régimen que se acaba de establecer en Chile, que, al menos a primera vista, considera *menos* restricciones que las previstas para dicha medida intrusiva.

En efecto, hubiera sido de esperar que la medida estuviera sometida cuando menos a las mismas exigencias previstas en los arts. 222 y 226, pero el nuevo art. 225 bis solo exige que

> "existan fundadas sospechas basadas en hechos determinados, de que una persona ha cometido o participado en la preparación o comisión, o que el delito se esté cometiendo actualmente, o que se esté preparando la comisión o participación en una asociación delictiva o criminal".

Esto implica que, al menos en principio, la medida es procedente para la investigación de *cualquier delito* y no solo para la de crímenes, como es la exigencia general de las otras dos disposiciones. Adicionalmente, también en principio, podría dirigirse contra *cualquier usuario* de un equipo informático y no necesariamente contra el imputado, como exige el inciso segundo del art. 222, donde solo se equiparan al imputado personas que le sirven de intermediarias de comunicaciones o que le facilitan (a él o a sus intermediarios) sus medios de comunicación.

Respecto de lo primero (procedencia para la investigación de cualquier delito), se podrá argumentar, en favor de esta decisión, que el registro remoto es

simplemente un modo distinto de registrar un computador y que, si el registro físico de este es posible en cualquier procedimiento penal, con la sola condición de que se cuente con una orden judicial, sea que el registro se verifique *in situ*, sea, como será la regla, que se lo incaute y se lo registre luego en otro lugar (arts. 205 y 217), no habría razón para establecer un régimen distinto. Pero con esto se pasaría por alto que, a diferencia de lo que ocurre con un registro convencional[15], aquí se trata explícitamente de una medida *subrepticia*, con lo cual la intensidad de la medida en términos de intromisión es mucho mayor[16]. Esto debiera llevar a los tribunales a ser especialmente estrictos a la hora de conceder las autorizaciones, aunque debe reconocerse que la ley no parece dejar espacio para no conceder la autorización en base a criterios de proporcionalidad si se dan los presupuestos de procedencia de la medida[17], esto es, la existencia

[15] Si ha sido precedido por la incautación del equipo informático esto es sencillamente evidente, pero también debiera serlo en los demás casos, por la regulación del registro en los arts. 205, 212 y 216, que sugieren que se trata de una medida ostensible. Es cierto que el art. 212 permite prescindir de la notificación al dueño o encargado y de la invitación a él a presenciar el acto, "sobre la base de antecedentes que hicieren temer que ello pudiere frustrar el éxito de la diligencia", pero nada más en la regulación sugiere que pueda ser una medida subrepticia, sin que, por otra parte, el art. 236 pueda servir de base suficiente para entradas y registros ocultos, porque este supone que la falta de comunicación al afectado, por la naturaleza de la diligencia, "resulta indispensable para su éxito". Es cierto que la falta de comunicación al afectado puede fundarse, alternativamente, también en la gravedad del hecho, pero en tal caso debiera proceder en casos más bien excepcionales, al margen de que sigue siendo muy dudoso que realmente se puedan implementar registros físicos subrepticios sobre una base normativa tan escueta. Hasta donde se puede ver, nunca se han practicado registros físicos bajo esa modalidad en nuestra práctica. En el derecho alemán, precisamente a propósito de una solicitud de autorización de registro informático remoto con invocación de las reglas generales sobre entrada y registro (antes de la introducción del § 100b StPO), se resolvió que la autorización no era procedente, no por el carácter remoto de la medida, sino fundamentalmente por su carácter subrepticio (sentencia del Tribunal Supremo Federal, de 31 de enero de 2007, BGHSt 51, 211).

[16] La mayor intensidad de un registro convencional subrepticio se reconoce aun en la práctica judicial estadounidense, donde la autorización judicial de esta modalidad (*sneak and peek search warrants*, más formalmente: *delayed notice search warrants*) ha estado tradicionalmente asociada a más exigencias en el escrutinio judicial. Cabe mencionar que debió preverse explícitamente en las Reglas Federales del Procedimiento Penal, Regla 41(f)(3) y que debe enviarse anualmente un informe al Congreso sobre su aplicación, conforme a la USA Patriot Act, 18 U.S.C. § 3103a(d)(2).

[17] Ni el art. 5º (referido a la interpretación de la ley, no a las circunstancias del caso que debe resolverse), ni el art. 9º (que solo establece la necesidad de autorización y la competencia para ello), establecen un mandato general de ajustarse al principio de proporcionalidad, el que solo parece recogido siquiera implícitamente en disposiciones dispersas (por ejemplo, el art. 222, además de la restricción formal, exige para la interceptación que "la investigación de tales delitos lo haga imprescindible"). No se descarta que un mandato en ese sentido se

de las fundadas sospechas basadas en hechos determinados a que se refiere el art. 225 bis.

Ahora bien, el asunto es completamente distinto si el registro, por las características concretas del programa informático a utilizar, permite acceder a las comunicaciones del usuario *en tiempo real*, esto es, en el momento en que está enviando o recibiendo mensajes de cualquier tipo o formato (sobre esto, *supra* 1), porque en tal caso y en esa exacta medida, constituye una interceptación en los términos del art. 222 y solo procede respecto de la investigación de crímenes o de simples delitos para cuya investigación está excepcionalmente previsto. Esto, por cierto, al margen de ser *también* un registro informático remoto en los términos del art. 225 bis, porque, en cuanto el registro sirve en el caso concreto como medio para la interceptación, realiza con ello, al mismo tiempo, los presupuestos conceptuales de ambas medidas, y teniendo estas requisitos de distinto nivel, en concreto deben satisfacerse necesariamente los más exigentes. De lo contrario, como es obvio, la solicitud de autorización para una medida menos intensa, solo porque en efecto tendrá lugar, serviría

---

pueda construir interpretativamente, pero eso supondría un esfuerzo de justificación que no puede intentarse aquí. Sería deseable una disposición que obligara siempre al juez a valorar si la medida es en concreto, atendidas las circunstancias del caso, conducente, estrictamente necesaria y no desproporcionada, aunque, ojalá, sin caer en el impropio y exasperante estilo de manual universitario de la legislación española, específicamente del art. 588 bis a LECr, el primero del Capítulo IV del Título VIII del Libro II, referido específicamente a las medidas intrusivas tecnológicas: "Principios rectores. 1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. 2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva. 3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad. 4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida. 5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

como sencillo expediente para eludir los requisitos de la autorización de otra medida más intensa que también tendrá lugar a través de ella. Lo decisivo no es la forma o la disposición legal invocada, sino exclusivamente la naturaleza de la medida concreta.

Se podría objetar que, siendo la afectación de esas comunicaciones una mera eventualidad, no hay razones para excluir *a priori* el registro remoto en la investigación de simples delitos. Esto puede ser, sin duda, correcto, pero solo a condición de que el Ministerio Público, al fundar su solicitud, exponga cómo es que el registro no implicará en concreto una intromisión en las comunicaciones del usuario del equipo informático afectado por la medida. De lo contrario, se estaría autorizando genéricamente una interceptación de comunicaciones inútil, permitiendo gratuitamente, en consecuencia, una afectación grave de las garantías fundamentales de una persona. Es cierto que los resultados de una interceptación de comunicaciones, en casos en que ella no procede, no pueden ser aprovechados como prueba (art. 225), pero esta consecuencia no es más que un pobre remedio para una vulneración de garantías fundamentales que no debió haber tenido lugar, y cuya evitación es la razón de ser de la institución del juez de garantía. Como se sabe, no es imaginable una investigación penal efectiva sin cierto grado de afectación de garantías fundamentales, y la tarea precisa del juez de garantía es brindarle legitimidad a dicha afectación, asegurándose de que, además de estar permitida siquiera *prima facie*, es estrictamente necesaria para los fines de la investigación, que es lo único que puede justificarla. Entonces, al margen de que para la persona cuyas garantías han sido conculcadas no puede ser consuelo suficiente que aquello no la perjudicará aún más (en términos de consecuencias penales), resultaría sencillamente irracional y contrario a la lógica interna del sistema legal que se permitiera genéricamente (y ese es el caso si la medida en concreto permite enterarse sin más de ellas en tiempo real) que a una persona le intercepten sus comunicaciones, cuando se sabe de antemano que eso, en cuanto no es aprovechable, no puede servirle a la investigación.

En consecuencia, será tarea del Ministerio Público demostrar que el registro remoto en concreto no constituirá una interceptación de comunicaciones en los términos del art. 222. Si los programas disponibles para la medida permiten una intromisión diferenciada, ciertamente no habrá impedimento legal (al margen de que resulte injustificadamente desproporcionado, como ya se ha dicho) para autorizar la medida, respecto de aquello que no constituye comunicación en tiempo real del usuario, en el contexto de la investigación de un simple delito. Ahora bien, si los programas disponibles no permiten esa intromisión diferenciada, el Ministerio Público solo podría obtener una autorización en contextos que no permitan solicitar la interceptación de comunicaciones si convence en cuanto a que la aplicación del programa se verificará de un modo y en unas circunstancias tales que excluyen o al menos minimizan radicalmente

la posibilidad de que se acceda en concreto a comunicaciones en tiempo real del usuario del equipo. En mi opinión, esto solo sería posible, si se trata de una intromisión que dure lo estrictamente necesario para hacerse del contenido del equipo en un momento dado, siempre que este tiempo sea lo suficientemente breve como para que, en conjunto con otras circunstancias, como el horario de la intromisión o la ausencia del usuario en el lugar donde se encuentra el equipo, con la consiguiente falta de acceso a él, en efecto se pueda descartar o minimizar la posibilidad de acceso en tiempo real a sus comunicaciones[18].

En otras palabras, para tener que satisfacer solo las exigencias del registro remoto y no las de la interceptación, la medida debiera ser un símil del registro convencional (en este caso, subrepticio), en cuanto intromisión puntual y temporalmente acotada (al margen de que excepcionalmente pueda durar un tiempo considerable), cual no es el caso si tiene el carácter de una medida de *vigilancia*, que, por definición, es una intromisión cuya duración no está limitada por un objeto preciso distinto, pues consiste en permanecer o esperar deliberadamente en situación de enterarse de algo que puede ocurrir o no en el futuro. Y, cabe decir que, en esto, el registro remoto está claramente construido a imagen y semejanza de la interceptación y no del registro convencional, como se desprende de la circunstancia de que no se habla de la vigencia de la autorización, esto es, del tiempo dentro del cual debe tener lugar, como hace el art. 208 inciso segundo respecto de la entrada y registro, sino que de la *duración de la medida misma*[19], lo que no tiene ningún sentido si se trata de un acto puntual con un objetivo igualmente puntual. Al margen de que esto confirma la inconsistencia de la regulación legal, lo relevante es que, a menos que sea técnicamente posible una intromisión diferenciada, en casos de vigilancia remota se está indudablemente también ante una interceptación de comunicaciones, que solo es procedente en virtud de una autorización judicial dada bajo observancia de lo dispuesto en el art. 222.

[18] En cuanto se trata, en último término, solo de la minimización del riesgo de interceptación, es perfectamente posible que ese riesgo se realice contra lo previsto. Esto no afecta la legitimidad ni de la autorización ni de la medida, pero obviamente impide aprovechar el resultado de lo que constituye interceptación respecto de la investigación de delitos para la que no es admisible. Distinto es el caso cuando las circunstancias, en concreto, hacen que lo que debió ser, en el peor de los casos, excepcional, deje de serlo. En tal caso debería someterse nuevamente a la consideración del tribunal la procedencia de la medida.

[19] El inciso segundo del art. 225 bis dispone que la medida "será autorizada por un plazo máximo de 30 días" pudiendo llegar, con prórrogas, a uno de 60 días, mientras que, conforme al art. 225 ter letra f), la resolución que autoriza la medida debe especificar la "duración precisa de la medida.".

Algo similar se produce cuando se accede en tiempo real no ya a comunicaciones, sino a imágenes o sonidos a los que no se podría haber accedido de no mediar el registro remoto, en los términos del art. 226. La amplitud del término "imagen" permite incluir no solo las imágenes que el usuario vea en su navegación por internet (así como los registros de audio a los que acceda), incluyendo todo tipo de textos, sino también, incluso, los textos que él mismo genere o esté generando mientras dure la medida, con lo cual, también a su respecto deberían satisfacerse los requisitos más exigentes de dicho art. 226.

En síntesis, a pesar de la liviandad con que el legislador trató el registro remoto a la hora de establecer sus presupuestos de procedencia y legitimidad, en términos prácticos, en la medida en que su ejecución puede implicar en concreto una interceptación en los términos del art. 222 o una captación, grabación o registro en los del art. 226, será necesario muchas veces que en la especie se satisfagan los requisitos de ambos artículos, y no solo los menos exigentes del art. 225 bis, en particular que se trate de la investigación de un hecho constitutivo de crimen o de un delito considerado especialmente por la ley para estos efectos. Solo en aquellos casos en los que la tecnología permita una intromisión diferenciada que impida conocer en tiempo real procesos en que está involucrado el usuario o, de otro modo, se excluya o minimice drásticamente la posibilidad de una intromisión de esas características, bastará el cumplimiento de los requisitos de este último artículo.

Respecto de lo segundo (falta de precisión de la persona que puede ser afectada por la medida), es notable que la ley haya tomado este resguardo respecto de una medida que *por definición* afectará a terceras personas (todos aquellos que se comuniquen con el imputado o las personas equiparadas), y que no haga lo mismo respecto de una medida respecto de la cual en muchos casos, al menos en principio, se puede identificar sin dificultades a la persona específica contra la que se dirige la medida. Con todo, puede entenderse también que la preocupación expresada en el art. 222 (tomada probablemente del derecho alemán[20], que respecto de cada medida intrusiva expresa contra quien se puede dirigir, con alcances diferenciados en algunos casos), resulta exagerada, porque debiera entenderse sin más que si la ley exige que existan "fundadas sospechas basadas en hechos determinados" contra una persona también determinada, ha

[20] La norma vigente en Chile ya estaba considerada en el Anteproyecto (art. 310), con referencias al art. 167 del Código Procesal Penal modelo para Iberoamérica, que simplemente se remite y ordena la aplicación analógica de la incautación de correspondencia, a los arts. 266 y 267 del Código italiano, que no se refieren al punto, y a los §§ 110a y 110b StPO. Las referencias del Anteproyecto pueden verse en Londoño, Fernando *et al*. *Reforma Procesal Penal. Génesis, historia sistematizada y concordancias*, T. II. Santiago: Editorial Jurídica de Chile (2003), pp. 220 y ss.

de entenderse, aunque la ley no lo explicite, que la medida solo puede dirigirse contra ella. Con esto, en vez de un exceso, podría más bien apreciarse un defecto, pues no habría cobertura legal para dirigir la medida contra personas distintas del imputado, en casos calificados en que esto se justificara, por ejemplo, porque hay razones suficientes y atendibles para suponer que el imputado o sujetos vinculados a él se valen de un equipo ajeno para los efectos que son de interés para la investigación. La parquedad de la ley permite que jueces atentos puedan administrar la medida razonablemente, permitiéndola por regla generalísima solo contra el imputado, pero también contra terceros, en casos excepcionales y calificados, como se acaba de mostrar.

Un asunto distinto, no tratado por la ley, es cómo debe procederse cuando un equipo tiene más de un usuario, con lo cual la medida puede afectar a personas respecto de las cuales no existe sospecha alguna. Si bien esta circunstancia no debiera, en principio, impedir la aplicación de la medida, pues es un riesgo inevitable de cualquier medida intrusiva que se afecte a terceros (en una interceptación telefónica se afecta a cualquier persona que llame al aparato intervenido o sea llamada desde él, aunque no tenga ninguna relación con los hechos investigados; en un allanamiento se puede afectar a un familiar, amigo o vecino que pidió le guardaran un objeto, etc.), pero, ante el menor estándar de garantías dispuesto por el legislador, la circunstancia indicada y la idea de que, en principio, la medida solo puede dirigirse contra el imputado, puede servir como base para un juicio acotado de proporcionalidad, negándose la autorización cuando los resultados que promete la medida no justifiquen una vulneración tan intensa de los derechos de terceros.

4. Situación de los llamados "datos de tráfico" y similares

Normativa aplicable

Art. 218 ter. *Registros de llamadas y otros antecedentes de tráfico comunicacional.* Cuando existan fundadas sospechas basadas en hechos determinados y ello sea útil para la investigación, el Ministerio Público podrá requerir a cualquier proveedor de servicios, previa autorización judicial, que entregue la información que tenga almacenada relativa al tráfico de llamadas telefónicas, de envíos de correspondencia o de tráfico de datos en internet de sus abonados, referida al período de tiempo determinado en la resolución judicial.

Para efectos de este artículo se entenderá por datos relativos al tráfico todos aquellos referidos a una comunicación realizada por medio de un sistema informático o de telecomunicaciones, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la

hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

El Ministerio Público podrá requerir, en el marco de una investigación penal en curso y sin autorización judicial, a cualquier proveedor de servicios que ofrezca servicios en territorio chileno, que facilite los datos de suscriptor que posea sobre sus abonados, así como también la información referente a las direcciones IP utilizadas por éstos para facilitar la identificación de quienes corresponda en el marco de la investigación. Los proveedores de servicios deberán mantener el secreto de esta solicitud.

Por datos de suscriptor se entenderá aquella información que posea un proveedor de servicios relacionada con sus abonados, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, tales como la información del nombre del titular del servicio, número de identificación, domicilio, número de teléfono y correo electrónico. Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de un año, una nómina y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios.

Los funcionarios públicos, los intervinientes en la investigación penal y los empleados de las empresas mencionadas en este artículo que intervengan en este tipo de requerimientos deberán guardar secreto acerca de ellos, salvo que se les cite a declarar.

La entrega de los antecedentes deberá realizarse en el plazo que disponga la resolución judicial. Si el requerido estima que no puede cumplir con el plazo en atención al volumen y la naturaleza de la información solicitada o la información no existe o no la posee, deberá comunicar dicha circunstancia fundadamente al tribunal, dentro del término señalado en la resolución judicial respectiva.

Si a pesar de las medidas señaladas en este artículo la información no es entregada, podrá ser requerida al representante legal de la institución u organización de que se trate, bajo apercibimiento de arresto.

La infracción a la mantención de la nómina y registro actualizado de los antecedentes a que se refiere el inciso cuarto será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley Nº 18.168, General de Telecomunicaciones. El incumplimiento de las obligaciones de mantener con carácter reservado y adoptar las medidas de seguridad correspondientes de los antecedentes señalados en dicho inciso, será sancionado con la pena prevista en la letra f) del artículo 36 B de la ley Nº 18.168. Los registros así obtenidos quedarán bajo custodia del Ministerio Público, quien cuidará que los datos en cuestión no sean conocidos por terceras personas.

> Los registros sólo podrán ser utilizados para los efectos de la investigación en la que fueron solicitados, u otras seguidas por delitos que merezcan pena de crimen o sean propias del sistema de análisis criminal y focos investigativos, de acuerdo con lo establecido en el artículo 37 bis de la ley Nº 19.640, que establece la ley orgánica constitucional del Ministerio Público, y no podrán ser utilizados para otros fines.
> El ejercicio de esta facultad se regulará mediante instrucciones generales dictadas por el Fiscal Nacional, conforme a lo establecido en el artículo 17 letra a) de la ley Nº 19.640, con el objeto de asegurar su uso racional.

El propósito legislativo detrás del nuevo art. 218 ter era regular de modo sistemático el acceso a datos relativos a una comunicación, pero distintos de su contenido comunicativo, en principio, genéricamente, "datos de tráfico". Como hacía presente la asesora de la Subsecretaría del Interior en segundo trámite constitucional ante el Senado, la indicación del Ejecutivo referida expresamente a "Registros de llamadas y otros antecedentes de tráfico comunicacional" y que sometía la obtención de esos datos sin distinción a la exigencia de autorización judicial (art. 218 bis), se buscaba hacer orden y claridad sobre una materia que en la práctica recibía tratamientos dispares, pues, en efecto, en algunos casos el Ministerio Público los pedía directamente a las empresas de comunicaciones y en otros se entendía que se requería una autorización judicial[21]. Posteriormente, otra indicación del Ejecutivo propuso una regulación más amplia, que, entre otros elementos, introducía la distinción entre *datos de tráfico* propiamente tales y *datos de suscriptor*, sometiendo la obtención de ambos al requisito de autorización judicial (art. 218 ter)[22], aspecto que, finalmente fue modificado, manteniendo dicho requisito solo para los datos de tráfico propiamente tales, de nuevo a propósito de una indicación del Ejecutivo[23].

Tal como es usual en el derecho comparado, en consecuencia, se pasa a distinguir entre datos de tráfico (o relativos al tráfico) propiamente tales y datos de suscriptor.

Los *datos de tráfico* son aquellos "referidos a una comunicación realizada por medio de un sistema informático o de telecomunicaciones, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la

[21] Segundo Informe de Comisión de Seguridad Pública del Senado, de 20 de enero de 2023, HL Nº 21.577, p. 289 (la propuesta en p. 288).

[22] Segundo informe, cit., HL Nº 21.577, p. 291, la indicación, defendida en su momento por el Encargado Nacional de Ciberseguridad y fustigada por el director de la ULDDECO del Ministerio Público (ambos en p. 292), fue retirada por el Ejecutivo.

[23] Segundo informe, cit. HL Nº 21.577, p. 294 s.

comunicación o el tipo de servicio subyacente", aclarando la ley que se trata de este tipo de información en relación con "llamadas telefónicas... envíos de correspondencia o [...] de datos en internet", con lo cual queda claro que la medida no incide solo en las comunicaciones privadas, sino también en otras esferas de la vida privada. Como se puede ver, se está frente a información que, si bien puede no ser tan sensible como el contenido mismo de la comunicación, permite, sobre todo gracias al desarrollo tecnológico, conocer mucho más sobre el titular del equipo (asumiendo que sea él quien en concreto lo usa) que lo que en el pasado era posible. Esto explica que el legislador chileno haya optado por someter la obtención de estos datos por parte del Ministerio Público a la exigencia de autorización judicial previa, aunque sin las limitaciones adicionales que impone a la interceptación de comunicaciones (inciso primero).

Esto está en consonancia con lo que se observa en el derecho comparado, donde en general se requiere autorización judicial para acceder a estos datos. Esa es la solución en los Estados Unidos, conforme a los Capítulos 121 (18 U.S.C. §§ 2701 ss.) y 206 (18 U.S.C. §§ 3121 ss.) del U.S.C., a pesar de que en *Smith v. Maryland*, 442 U.S. 735 (1979) se declaró que dichos datos no están cubiertos por la protección de la Cuarta Enmienda de la Constitución de los Estados Unidos; también en el derecho español, en el art. 588 ter j LECr, sobre datos obrantes en archivos automatizados de los prestadores de servicios; y también en el caso alemán (§ 100g StPO), si bien aquí rodeado de garantías inusitadas que merecen una explicación adicional: mediante Ley de 10 de diciembre de 2015 (BGBl I, 2218), luego de que se declarara inconstitucional el régimen establecido previamente[24], se introdujo un nuevo régimen legal que, dentro

[24] Mediante Ley de 21 de diciembre de 2007 (BGBl I, 3198), que trasponía al derecho alemán la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, se introdujeron en la Ley de Telecomunicaciones (TKG) artículos que imponían a las empresas proveedoras de telecomunicaciones el almacenamiento de los datos de tráfico de sus clientes, por seis meses, a disposición de los órganos de persecución penal (§§ 113a y 113b TKG), mientras que el acceso a ellos por parte de estos órganos estaba regulado en el § 100g StPO, que también fue modificado. Esta regulación fue declarada inconstitucional por sentencia de 2 de marzo de 2010, en lo fundamental, por ser incompatible, en opinión del Tribunal Constitucional Federal (BVerfG), con el Art. 10 de la Constitución (secreto de las comunicaciones), en ausencia de razones concretas que justificaran el almacenamiento masivo de datos personales por un período tan extenso, además de objetarse la parquedad de la regulación de la ley en cuanto a seguridad de los datos, su uso, transparencia y remedios legales a disposición de los afectados (BVerfGE 125, 260). Cabe mencionar que, con posterioridad, a solicitud del Tribunal Superior de Irlanda y del Tribunal Constitucional de Austria, el Tribunal de Justicia de la Unión Europea revisó la validez de la mencionada Directiva 2006/24/CE y la invalidó, mediante sentencia de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12. Con todo, la invalidación en ambos casos se debe, fundamentalmente, a la extensión y condiciones del deber previo de los proveedores de mantener disponible los datos.

de los datos de tráfico propiamente tales, distingue entre dos tipos de datos: por una parte, aquellos que es indispensable conservar por un cierto tiempo, generalmente acotado, para los efectos de que las compañías puedan hacer posibles las comunicaciones y calcular el consumo que sirve de base para cobrar por sus servicios (§ 9 de la Ley de protección de datos y de la esfera privada en la telecomunicación y medios a distancia, TTDSG), así como para detectar, limitar y corregir fallas de servicio o para descubrir o impedir usos ilícitos del servicio (§ 12 TTDSG); y, por la otra, aquellos datos de tráfico que deben conservarse a disposición de los órganos de persecución penal (§ 176 de la Ley de Telecomunicaciones, TKG). En el proceso penal, el acceso a los primeros (supuesto que aún estén disponibles) es posible respecto de la investigación de delitos de relevancia, pero sin referencia a un catálogo taxativo (lo mismo rige para la obtención del número de aparato de un teléfono móvil o de la tarjeta utilizada, así como de la ubicación de un teléfono móvil, de acuerdo con el § 100i StPO), mientras que el acceso a los segundos, que ahora deben conservarse por solo 10 semanas, salvo los más sensibles que permiten la localización de un sujeto (*Standortdaten*), para los cuales rige un plazo de apenas 4 semanas, está sometido al régimen más estricto de todos los que se conocen en materia de medidas tecnológicas de investigación, pues solo procede respecto de la investigación de delitos contenidos en un catálogo muy acotado (básicamente de delitos muy graves que afectan bienes jurídicos personalísimos o bienes jurídicos institucionales esenciales)[25]. Respecto de datos de uso de medios telemáticos, se prevé una regulación muy similar en el § 100k StPO. Estas dos medidas no solo requieren autorización judicial, sino que, además, en principio y a diferencia de la mayoría de las medidas precedentemente presentadas, deben ser comunicadas previamente a los afectados. En ese escenario, la decisión legal chilena parece moderada y correcta.

Por su parte, los llamados *datos de suscriptor* consisten en la información que sobre sus abonados o suscriptores posee un proveedor de servicios y "que permita determinar su identidad, tales como la información del nombre del titular del servicio, número de identificación, domicilio, número de teléfono y correo electrónico", "excluidos los datos sobre tráfico y contenido" de las comunicaciones. Estas informaciones básicas de la relación contractual entre suscriptor y empresa pueden ser requeridos directamente a las empresas por

[25] Sobre el contexto de surgimiento del nuevo precepto, Henrichs, Simon; Weingast, Karin. "§ 100g StPO", en Barthe, C.; Gericke, J. (eds.). *Karlsruher Kommentar zur Strafprozessordnung*, 9º ed., München: Beck (2023), nº marg. p. 1 ss.; en español, véase Rolón, Darío N. "Acceso procesal a datos alojados en el proveedor de servicios de telecomunicaciones (TSP) según la Ordenanza procesal penal alemana", en *Revista de Estudios de la Justicia*, Nº 23 (2015), pp. 145 ss.

el Ministerio Público, explícitamente sin necesidad de autorización judicial, y debiendo mantenerse en secreto el requerimiento a su respecto (inciso tercero).

También en esto la solución chilena parece concordante con el derecho comparado. Así, por ejemplo, es la misma solución del derecho español en el art. 588 ter m LECr, sobre identificación de titulares o terminales o dispositivos de conectividad, y en los Estados Unidos, conforme a la sección 2703 del Título 18 del U.S.C.

Los problemas de la regulación provienen de la desordenada técnica legislativa a través de la cual se expresa el modelo recién descrito. Es cierto que no es de esperar un problema interpretativo a partir del hecho de que, al disponerse en el inciso tercero la entrega no sujeta a autorización judicial de los datos de suscriptor, se disponga lo mismo, como si fuera algo diferente, respecto de "la información referente a las direcciones IP utilizadas" por los abonados, en circunstancias en que estos debieran considerarse ya incluidos en el concepto de datos de suscriptor. Pero la lectura se complica cuando, al establecerse en el inciso cuarto el deber de las empresas que prestan servicios de telecomunicaciones e internet de mantener a disposición del Ministerio Público cierta información a efectos de una investigación penal, parecen mezclarse ambos tipos de datos, pues, por un lado, se habla de una nómina y registro actualizado de sus "rangos autorizados de direcciones IP" de sus clientes o usuarios, así como sus "domicilios o residencias", pero también los números IP "de las conexiones que realicen", que serían, en rigor, datos de tráfico, agregándose explícitamente que esto debe conservarse "con sus correspondientes datos relativos al tráfico", todo eso, con carácter reservado y adoptando las medidas de seguridad correspondientes, por el plazo de un año[26].

Por cierto, puede entenderse que una cosa es el deber de las empresas de conservar cierta información y otra el modo en que el Ministerio Público puede acceder a ella en cada caso, para lo que sería decisiva la naturaleza de los datos en cuestión, conforme al esquema recién descrito. Aquí se está por aceptar esta lectura, que parece ser la única consistente con la introducción de la distinción por tipos de datos en la ley, pero no puede desconocerse que la circunstancia de que se establezca que todos estos datos, sin distinción, deben conservarse "a disposición del Ministerio Público" es cuando menos equívoca, pues no parece que se pueda decir que algo está a disposición del Ministerio Público cuando este organismo solo puede acceder a ello cuando un juez tiene

[26] Solo a la pasada, no puede dejar de llamarse la atención en cuanto a que, como se acaba de indicar, un deber genérico de este tipo, y por la mitad del tiempo que rige en Chile, fue declarado incompatible con la Constitución en Alemania y dio lugar a la invalidación de una Directiva de la Unión Europea por el TJUE, a requerimiento de autoridades irlandesas y austriacas.

a bien aprobarlo. Máxime si una formulación prácticamente idéntica en el inciso quinto (ahora sexto) del art. 226, sin referencia alguna a la necesidad de autorización judicial[27], servía de argumento precisamente para entender que el Ministerio Público podía requerir directamente esos datos, al margen de que, como se dijo, la práctica no era uniforme. Y lo más desconcertante es que se haya introducido un nuevo art. 218 ter, con el propósito declarado de regular sistemáticamente la materia de estos datos distintos del contenido de una comunicación, y no se haya removido este antecedente en el art. 222, con lo cual podría aun sostenerse que, para los efectos de preparar una solicitud de autorización de una interceptación de comunicación, la situación, regida aún por un art. 222 que no se vio alterado en esta parte, sigue siendo dudosa, si no abiertamente la contraria a la establecida en el nuevo precepto. Con todo, al margen de la chapucería legislativa, debe insistirse en que lo único coherente con la introducción en la ley de la distinción entre datos de tráfico y datos de suscriptor es asumir que, al margen de los derechos de conservación que puedan pesar sobre las empresas, la forma en que puede acceder a ellos el Ministerio Público es la prevista en los incisos primero y tercero: autorización judicial para los primeros, requerimiento directo para los segundos.

Más allá de los requisitos que deben cumplirse para la procedencia y legitimidad de la medida, de las múltiples obligaciones que impone la regulación, solo parecen ser de relevancia para la cuestión sobre la admisibilidad de los antecedentes que se obtengan gracias a ella como prueba, directa o mediata, en un juicio penal, las que dicen relación con el tiempo máximo previsto para que ciertas informaciones estén disponibles para el Ministerio Público. En efecto, el incumplimiento de los deberes concernientes a la confidencialidad y a la seguridad del almacenamiento, sea por parte de la empresa o del Ministerio Público, puede dar lugar sin duda a responsabilidad de aquella o de este o, en fin, del Estado, pero no parece que pueda sostener la afirmación de haberse obtenido con inobservancia de garantías fundamentales, en los términos del inciso tercero del art. 276. En cambio, si la información a que accedió el Ministerio Público era una información de aquella que se debía conservar exclusivamente para estar disponible para eventuales necesidades del proceso penal y esta se conservó más allá del tiempo máximo previsto, al cabo del cual lo que corresponde es la destrucción de los datos, bien puede verse en dicha

[27] Mediante la Ley Nº 19.927, de 14 de enero de 2004, se estableció que las empresas debían "mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a seis meses, de los números IP de las conexiones que realicen sus abonados", plazo que la Ley Nº 20.526, de 13 de agosto de 2011, elevó a un año. El resto de las modificaciones del precepto, incluidas las debidas a la Ley Nº 21.577 no han alterado este cuadro.

conservación una vulneración de la esfera privada del afectado y, con ello, un caso de prueba que debe ser excluida de acuerdo con el referido inciso tercero del art. 276, por las razones que se pasan a exponer.

Lo primero que se debe destacar es que el plazo de un año previsto por el inciso cuarto es el mismo previsto desde el 2011 y con el mismo objeto por el (ahora) inciso sexto del art. 222. Lo curioso (¡nueva rareza legislativa!) es que el destino de los datos al cabo de ese plazo no está previsto en la flamante regulación sistemática sobre la materia, sino que en el viejo art. 222 *aggiornato*. En efecto, se debe precisamente a la Ley Nº 21.577 haber insertado la siguiente oración en el (ahora) inciso sexto:

> "Transcurrido el plazo máximo de mantención de los datos señalados precedentemente, las empresas y prestadores de servicios deberán destruir en forma segura dicha información".

Lo llamativo es que, por primera vez, la ley chilena habla de un plazo *máximo*, y esto es de extraordinaria importancia conceptual. Porque todo sugiere que, originariamente, desde el punto de vista de la investigación penal, se trataba de un plazo *mínimo* garantizado para poder contar con la información, ya que, en rigor, no se veía problema alguno en que las empresas conservaran incluso a perpetuidad datos personales de sus abonados. Más bien el problema era que ellas no tenían ningún interés en conservar la información, por razones prácticas y de costos, de modo que de lo que se trataba era de obligarlas a hacer algo que no habría querido hacer voluntariamente, y esto por un tiempo mínimo razonable desde la perspectiva de la persecución penal[28].

Pero es obvio que con los años la conservación indiscriminada de los datos empieza a verse de un modo distinto, como lo es también que surgió un interés distinto y antagónico, como es la protección de los datos personales. Desde esa perspectiva específica, la conservación indiscriminada de todos los datos de tráfico asociados de dispositivos de una persona por un año ciertamente representa una afectación de la vida privada de las personas, para la cual hay, sin duda, buenas razones que la justifican; pero el establecimiento de un plazo máximo, que desde el punto de vista de los derechos de los abonados es efectivamente el máximo por el que están obligados a tolerar esa afectación, define al mismo tiempo, al menos en principio, los requisitos de la legitimidad posible del acceso a esos datos. Por cierto, puede discutirse si el plazo de un año previsto por la ley es razonable o no, por exceso o por defecto, y hay buenas razones

[28] Nótese que, durante la tramitación legislativa, el Fiscal Nacional del Ministerio Público echaba en falta que no se discutiera sobre el punto, a la vez que afirmaba que el plazo era insuficiente y sugería ampliarlo "al menos" a tres años, como habría ocurrido en otros países. Informe de la Comisión de Seguridad Ciudadana de la Cámara de Diputados, de 5 de mayo de 2021, HL Nº 21.577, p. 47.

para pensar que, por ejemplo, los plazos del derecho alemán (diez y cuatro semanas, según el tipo de dato de crédito), son extremadamente breves. Pero no es el punto. El punto es que la decisión concreta del legislador respecto de los requisitos para la afectación legítima de una garantía fundamental, en este caso el respeto y protección de la vida privada, de acuerdo con el art. 19 Nº 4 de la Constitución, es la referencia obvia del inciso tercero del art. 276 para los efectos de la exclusión de prueba.

Si bien el debate al respecto fue más bien acotado durante la tramitación de la Ley Nº 21.577, fue mucho más intenso cuando se discutió la que llegaría a ser Ley Nº 21.459, de 20 de junio de 2022 (Boletín Nº 12.192-25). Así, por ejemplo, el informe preceptivo de la Corte Suprema sobre el proyecto, a propósito de la propuesta de aumentar a dos años el plazo (mínimo) durante el cual las empresas debían mantener los datos de tráfico de sus clientes, hizo presente que:

> "esta regulación parece exceder un criterio de proporcionalidad razonable y, en la medida de que afecta la intimidad de las personas, no [sic] satisfacería los requerimientos mínimos que debe cumplir una medida de esta clase, especialmente, al no [sic] estipular un horizonte máximo tras el cual los datos debiesen ser borrados. No debe perderse de vista que, tal como han enseñado los últimos escándalos internacionales sobre la materia, el procesamiento de meta-data no sólo permite obtener información privada de gran sensibilidad para las personas, sino que permite manipulaciones a gran escala que constituyen un peligro para la democracia".

Y, luego de referirse a la ya mencionada invalidación por parte del TJUE de las disposiciones de la Directiva 2006/24/CE, al Informe del año 2017 de la Relatoría Especial para la Libertad de Expresión en el sistema interamericano y a la Resolución 68/167 de la Asamblea General de las Naciones Unidas, de 18 de diciembre de 2013, sobre "El derecho a la privacidad en la era digital", concluye en los siguientes términos:

> "Que frente a esta modificación solo cabe hacer presente que conforme a los estándares internacionales de derechos humanos, cualquier clase de injerencia o afectación de derechos fundamentales, debe dar cumplimiento a las condiciones que ha identificado la Corte Interamericana de Derechos Humanos en el sentido de satisfacer los principios de legalidad, legitimidad del fin, idoneidad, necesidad y proporcionalidad de la medida. Lo cierto es que una medida de esta clase, sin límite máximo temporal para la retención de datos, no satisface los criterios de necesidad y proporcionalidad de la medida, independientemente de la legitimidad del fin que persiguen"[29].

[29] Informe de 12 de febrero de 2018, Historia de la Ley Nº 21.459, considerandos 21º y 22º, p. 48 s.

Ahora bien, en definitiva el legislador de la Ley Nº 21.577 ratificó, para bien o para mal, que el plazo de conservación de un año que venía desde antes era adecuado, pero lo concibió explícitamente como un plazo máximo, lo que solo se entiende desde el punto de vista de los derechos y garantías de los abonados, que ven afectada su vida privada por dicha conservación. De esto se sigue, necesariamente, que el acceso a datos de tráfico de clientes que una empresa proveedora de servicios de telefonía o internet ha conservado a disposición del Ministerio Público *más allá* del plazo máximo previsto por la ley, tiempo al cabo del cual, según la misma ley, debió haberlos destruido en forma segura, no por mor de reducir sus costos, sino de resguardar la protección de los datos personales de sus clientes, constituye una inobservancia de garantías fundamentales en los términos del inciso tercero del art. 247 y debiera dar lugar a la exclusión de la prueba obtenida directa e indirectamente a partir de dicha inobservancia.

Naturalmente, la situación es distinta cuando se trata de información que se requiere conservar con base a antecedentes concretos y determinados contra una persona, es decir, cuando ya no se trata de una conservación indiscriminada sobre la base de un deber genérico, sino con fundamento en las reglas del proceso penal. Para que esto sea posible, sin embargo, se requiere que la información se solicite antes del vencimiento del plazo.

5. Excurso: la conservación provisoria de datos del art. 218 bis (Ley Nº 21.459)

Normativa aplicable

Art. 218 bis. *Preservación provisoria de datos informáticos.* El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquier proveedor de servicio, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia.

Cabe mencionar la función del nuevo art. 218 bis, introducido por la Ley Nº 21.549, de 20 de junio de 2022, y que entra a regir el 21 de junio de 2024. Esta norma sobre "preservación provisoria de datos informáticos", implementa en Chile lo dispuesto en el art. 16[30] del Convenio del Consejo de Europa sobre

[30] El art. 17 se refiere a lo mismo, pero en relación con los datos de tráfico, para lo cual, si bien este art. 218 bis puede ser aplicable, debiera ser desplazado por el art. 218 ter.

Cibercriminalidad (Convenio de Budapest de 2001). Se trata de la regulación de una verdadera medida cautelar, conforme a la cual el Ministerio Público está facultado para dirigirle con efecto vinculante un requerimiento directo a un proveedor de servicio (no a cualquier persona que los tenga, como prevé el Convenio), en orden a que conserve o proteja datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición, hasta que se obtenga la respectiva autorización judicial para su entrega (habrá que entender que conforme al inciso segundo del art. 217). Se establece un plazo de conservación de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días.

La disposición no debiera tener relevancia práctica respecto de datos de tráfico, cuyo acceso se regula de manera más completa y expedita en el art. 218 ter, en tanto que debe entenderse que lo que ella permite es sin perjuicio de las facultades del Ministerio Público para requerir derechamente la incautación de los datos, sea de modo convencional (art. 205), sea de modo remoto (art. 225 bis).

III. Análisis particular de las reglas sobre agentes encubiertos, agentes reveladores, informantes y entregas vigiladas, con especial referencia a los presupuestos de legalidad y legitimidad

Normativa aplicable

II. Agentes encubiertos, agentes reveladores e informantes

Art. 226 B. *Ámbito de aplicación.* El Fiscal Regional competente podrá autorizar a funcionarios policiales determinados para que se desempeñen como agentes encubiertos o agentes reveladores cuando sea necesario para lograr el esclarecimiento de hechos que involucren la participación en una asociación delictiva o criminal, establecer la identidad e intervención de sus responsables, conocer los planes de la asociación, y prevenir la comisión de sus delitos o comprobar los que hubieren cometido.

El Fiscal Regional deberá resolver la solicitud efectuada por el fiscal en un plazo máximo de 72 horas. En caso de negativa, el fiscal podrá solicitar nuevamente autorización para que funcionarios policiales se desempeñen como agentes encubiertos o agentes reveladores, aportando nuevos antecedentes.

No será necesaria la autorización establecida en el inciso primero, en aquellos casos en que sea el Fiscal Nacional o el Fiscal Regional quien dirija personalmente la investigación, conforme a lo establecido en los artículos 18 y 19 de la ley Nº 19.640.

Al autorizar la medida el Fiscal Regional deberá asegurarse que ella se limite a las acciones estrictamente necesarias para los objetivos de la investigación, que los agentes reveladores o infiltrados no induzcan a la perpetración de delitos, y

que la seguridad de los agentes reveladores o infiltrados se encuentra debidamente resguardada.

El acto que autorice la medida será mantenido en poder del Ministerio Público en dos registros distintos. Con todo, la información relativa a la verdadera identidad del agente se mantendrá únicamente en un registro.

La autorización deberá consignar, además, la identidad supuesta con la que actuará en el caso concreto, si la tuviere. Asimismo, el acto que autorice deberá:

a) Circunscribir el ámbito de actuación de dichos agentes en conformidad con los antecedentes y el delito o los delitos invocados en la solicitud correspondiente.

b) Expresar la duración de la autorización, la que no podrá exceder de sesenta días. Ella será prorrogable por períodos iguales, y deberá cumplir los mismos requisitos establecidos para su otorgamiento.

c) Establecer las medidas que deben adoptar para asegurar los objetivos establecidos en el inciso anterior, incluyendo aquellas previstas en el inciso cuarto del artículo 226 C.

Si se cumplen las mismas circunstancias indicadas en el inciso primero, el Fiscal Regional podrá autorizar a cualquier persona para que se desempeñe como informante.

Las autorizaciones establecidas en este artículo serán confidenciales y sólo podrán ser conocidas por terceros en los casos señalados en la ley.

Cuando la ley autorice el conocimiento por parte de terceros, el Ministerio Público pondrá a su disposición el registro que no consigna la información verdadera sobre la identidad de los agentes e informantes. El acceso al registro completo deberá ser autorizado por el juez de garantía competente con audiencia del Ministerio Público y se otorgará la autorización únicamente si es estrictamente necesario, si no pone en peligro la seguridad personal del agente o informante y si existen todas las medidas necesarias para que la información no llegue a terceros. Teniendo en consideración los antecedentes concretos, el juez podrá autorizar el acceso al registro total o parcialmente.

Art. 226 C. *Agente encubierto.* Agente encubierto es el funcionario policial que oculta su identidad oficial y se involucra o introduce en las asociaciones delictivas o criminales o agrupaciones u organizaciones a que se refiere el artículo anterior, con el objetivo de identificar a los participantes, reunir información y recoger antecedentes necesarios para la investigación.

El agente encubierto podrá tener una identidad e historia ficticias. La Dirección Nacional del Servicio de Registro Civil e Identificación deberá otorgar los medios necesarios para su oportuna y debida materialización. Los funcionarios policiales que han actuado en una investigación con identidad falsa podrán mantener dicha identidad cuando testifiquen en el proceso que pueda derivarse de los hechos en que hayan intervenido y siempre que así se disponga mediante resolución judicial fundada.

Asimismo, el Fiscal Regional podrá autorizar la apertura de una cuenta bancaria, la obtención de otras piezas de identidad relevantes tales como una licencia de conducir y la contratación de servicios básicos haciendo uso de la identidad ficticia. El uso de esta facultad se orientará exclusivamente a reforzar la credibilidad de la identidad e historia ficticias. Un reglamento expedido en conjunto por el Ministerio de Justicia y Derechos Humanos y el Ministerio del Interior y Seguridad Pública deberá establecer los procedimientos y condiciones de ejercicio de esta facultad.

Sin perjuicio de las penas aplicables por la perpetración de otros delitos, el uso manifiestamente indebido de las facultades asociadas a la historia ficticia será sancionado con la pena de presidio menor en su grado mínimo.

La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien solicitó la autorización de la medida.

Art. 226 D. *Agente revelador.* Agente revelador es el funcionario policial que simula requerir de otro la ejecución de una conducta delictiva con el objetivo de lograr la concreción de los propósitos delictivos de éste.

El agente revelador podrá tener una identidad e historia ficticias. La Dirección Nacional del Servicio de Registro Civil e Identificación deberá otorgar los medios necesarios para la oportuna y debida materialización de aquellas. Los funcionarios policiales que hubiesen actuado en una investigación con identidad falsa podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y siempre que así se acuerde mediante resolución judicial fundada.

La información que obtenga el agente revelador deberá ser puesta a la mayor brevedad posible en conocimiento de quien solicitó la autorización de la medida.

Art. 226 E. *Informantes.* Informante es quien suministra antecedentes sustanciales a los organismos policiales acerca de la preparación o de la comisión de un delito de asociación delictiva o criminal y requiere de protección.

La autorización que conceda la calidad de informante deberá ser otorgada por el Fiscal Regional.

Contando con autorización del Fiscal Regional, el Ministerio Público también podrá disponer que sea tratado como informante quien participe, con su conocimiento y bajo su control, de una operación encubierta o de una entrega vigilada.

III. Entregas vigiladas

Art. 226 F. *Ámbito de aplicación.* El Fiscal Regional podrá autorizar la entrega vigilada de objetos cuya fabricación, elaboración, distribución, transporte, comercialización, importación, exportación, posesión, o tenencia esté prohibida o restringida, o los objetos por las que se hayan sustituido total o parcialmente las anteriores mencionadas, de los instrumentos que hayan servido para la comisión de los delitos de que se trate, y de los efectos y ganancias de tales delitos, siempre

que ello resulte útil para la investigación de la participación en una asociación delictiva o criminal, o para establecer la identidad e intervención de intervinientes distintos de quienes se encuentran en posesión de los bienes en cuestión.
Se entenderá por entrega vigilada la técnica consistente en permitir que los objetos a los que se refiere el inciso anterior se trasladen, guarden, intercepten o circulen dentro del territorio nacional, salgan de él o entren en él, sin la interferencia de las policías o del Ministerio Público, pero bajo su conocimiento y vigilancia o control.
Al autorizar la medida, el Fiscal Regional deberá asegurarse que ella se limite a las acciones estrictamente necesarias para los objetivos de la investigación, que los agentes estatales no induzcan a la perpetración de delitos, que el procedimiento no ponga en riesgo la integridad personal de terceros y que los bienes cuya entrega vigilada se autoriza puedan ser, en definitiva, sujetos a comiso.
La resolución que autorice la medida deberá:
a) Delimitar el objeto de la entrega vigilada, así como el tipo y cantidad de las especies de que se trate.
b) Expresar la duración de la autorización, la que no podrá exceder de sesenta días, y será prorrogable por períodos iguales.
c) Establecer las medidas que deben ser tomadas para asegurar los objetivos establecidos en el inciso anterior.
Cuando los objetos se encuentren en zonas sujetas a la potestad aduanera, el Servicio Nacional de Aduanas observará las instrucciones que imparta el Ministerio Público para los efectos de aplicar esta técnica de investigación.
Cuando la entrega vigilada o controlada deba practicarse total o parcialmente en territorio extranjero, ella se ajustará a lo dispuesto en los acuerdos o tratados internacionales ratificados por Chile y que se encuentren vigentes, si los hubiere.
Art. 226 G. *Suspensión de la entrega vigilada.* Si las diligencias ponen en peligro la vida o integridad física de los funcionarios policiales o agentes encubiertos o reveladores que intervengan en la operación, la recolección de antecedentes relevantes para la investigación o el aseguramiento de los partícipes, el Ministerio Público podrá disponer la suspensión de la entrega vigilada y solicitar al juez de garantía que autorice la detención de los partícipes y la incautación de los instrumentos, objetos o efectos del delito.

IV. Disposiciones comunes

Art. 226 H. *Exención de responsabilidad criminal.* El agente encubierto, el agente revelador, el informante, así como los funcionarios que participen en una entrega vigilada u otra medida dispuesta de conformidad a este Párrafo, estarán exentos de responsabilidad criminal siempre que se trate de aquellos delitos en que deban incurrir o que no hayan podido impedir en cumplimiento de la resolución que autoriza la medida.

Art. 226 I. *Prohibición de la inducción a la perpetración de delitos.* El agente encubierto, el agente revelador y los funcionarios que participen en una entrega vigilada o en otra medida dispuesta de conformidad a este Párrafo, no podrán inducir a la perpetración de delitos que, de otro modo, no habrían sido cometidos por éste.

Art. 226 J. *Secreto y acceso a la información de defensa.* El Ministerio Público podrá disponer el secreto de determinadas actuaciones, registros o documentos respecto de uno o más intervinientes, cuando estime que existe riesgo para el éxito de la investigación o para la seguridad de los agentes encubiertos, agentes reveladores, informantes, testigos, peritos y, en general, de quienes hayan cooperado eficazmente en el procedimiento.

Se aplicará lo dispuesto en el artículo 182. Con todo, el Ministerio Público podrá disponer que se mantenga el secreto hasta el cierre de la investigación. Además deberá adoptar medidas para garantizar que el término del secreto no ponga en riesgo la seguridad de las personas mencionadas en el inciso anterior.

Tras el cierre de la investigación, el juez de garantía deberá procurar el acceso de la defensa a todos los medios de prueba pertinentes, y sólo lo restringirá en aquellos casos establecidos en el artículo 226 B, inciso final.

El que de cualquier modo informe, difunda o divulgue información relativa a una investigación amparada por el secreto, incurrirá en la pena de presidio menor en su grado medio a máximo.

Art. 226 K. *Extralimitación en el uso de técnicas especiales.* Los funcionarios policiales, agentes encubiertos y reveladores que ejecuten las medidas o actuaciones a que se refieren los artículos 226 B, 226 D y 226 F sin observar el objeto o límites impuestos por la autorización respectiva serán sancionados, además de las penas que corresponda por los delitos cometidos, con la pena de suspensión del empleo en su grado máximo y multa de quince a veinte unidades tributarias mensuales.

La misma pena se aplicará al fiscal que al ejecutar técnicas especiales imparta órdenes que impliquen un abuso en su ejercicio, en atención a lo autorizado por el Fiscal Regional o en la resolución judicial.

El juez de garantía declarará nulas las actuaciones que excedan manifiestamente el objeto de las técnicas especiales y las excluirá, de conformidad con el artículo 276.

El agente policial o fiscal del Ministerio Público que perpetre el delito del artículo 269 ter del Código Penal con ocasión del uso de las técnicas especiales referidas en el inciso primero, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo e inhabilitación especial perpetua para el cargo.

Art. 226 L. *Utilización de medios de prueba.* Los antecedentes o evidencia obtenidos mediante la aplicación de las facultades previstas en este Párrafo y que resulten irrelevantes para el procedimiento serán entregados o devueltos en su oportunidad a las personas respecto de quienes se solicitó la medida y se destruirá todo registro, transcripción o copia de ellos por el Ministerio Público.

> Lo prescrito en el inciso precedente no regirá respecto de aquellos antecedentes o evidencia que puedan ser útiles o relevantes para otros procedimientos seguidos por hechos en cuya investigación también sean aplicables las disposiciones de este Párrafo, delitos que merezcan pena de crimen o sean propias del sistema de análisis criminal y focos investigativos, de acuerdo con lo dispuesto en el artículo 37 bis de la ley Nº 19.640.
> Art. 226 M. *Rendición de cuentas.* El Fiscal Nacional deberá dar cuenta, anualmente, sobre el número de medidas especiales utilizadas de conformidad con este Párrafo, con la ley Nº 20.000 y con la ley Nº 19.913 y sobre sus efectos, tanto a la Comisión de Seguridad Pública del Senado como a la Comisión de Seguridad Ciudadana de la Cámara de Diputados, en sesiones que tendrán el carácter de reservadas.

Como ya se ha dicho, conforme al nuevo estatuto de las "técnicas especiales de investigación", estas, que hasta ahora solo eran aplicables en los pocos casos en que ello estaba especialmente previsto, lo son ahora para la investigación de cualquier delito, con tal que los hechos "involucren la participación en una asociación delictiva o criminal", lo que significa una ampliación muy considerable de su ámbito de aplicación.

Probablemente, la decisión política más relevante de la nueva regulación es que, a la hora de resolver si estas técnicas debían estar sometidas a la exigencia de autorización previa o no, se optó por el segundo camino. Como se recordará (*supra* I), no exigen esa autorización las regulaciones de las leyes especiales, particularmente el art. 25 de la Ley Nº 20.000, por remisión a este el art. 33 de la Ley Nº 19.913 o, también vía remisión, el art. 19 B de la Ley Nº 17.798, sobre control de armas, pero también (para la entrada vigilada) el art. 448 quáter CP; pero sí la requieren los arts. 369 ter y 411 octies CP y el inciso tercero del art. 12 de la Ley Nº 21.459, como también lo requería el suprimido art. 226 bis (y a través de este, en particular, el 448 septies CP). Pues bien, la Ley Nº 21.577 no elimina del todo estas diferencias de trato, pero avanza significativamente hacia una concepción de estas técnicas como actividad policial que, *por sí misma*, no implica afectación de garantías fundamentales.

Debe reconocerse que esta es la solución al parecer imperante en el derecho comparado de referencia usual. Así, en el derecho federal de los Estados Unidos, la acción de agentes encubiertos no está sometida a autorización judicial, sino solo a controles internos en la estructura del FBI, conforme a unas directivas que se revisan con cierta periodicidad[31]. En Alemania, en principio, solo se requiere conformidad del Ministerio Público (§ 110b I StPO), aunque

[31] *Undercover and Sensitive Operations Unit Attorney General's Guidelines on FBI Undercover Operations. Revised 11/13/92* (última versión disponible: 8 de marzo de 2017).

siempre que sea necesaria para la investigación de delitos de cierta relevancia en materia de tráfico ilícito de drogas o armas o de falsificación de moneda o sellos, o bien cuando se han cometido actuando profesional o habitualmente o como miembro de una banda (§ 110a StPO); con todo, se requiere autorización judicial cuando la investigación se dirige contra un imputado determinado o conlleva que el agente deba hacer ingreso mediando su identidad ficticia a lugares que no sean de acceso público (§ 110b II StPO). En cuanto a las entregas vigiladas, estas se consideran cubiertas por disposiciones generales relativas a la actividad policial, aunque hay previsión expresa (mas no regulación) en la Ley sobre cooperación internacional en materia penal (§ 91c II 2 c] bb] IRG). A nivel reglamentario, existen disposiciones específicas en los Nr. 29a a 29d de las Directivas para el procedimiento penal y contravencional del Ministerio de Justicia Federal, que regulan las relaciones entre policías y Ministerio Público. Si la medida se extiende en el tiempo (más de 14 horas continuadas o en más de dos días), debería aplicarse el § 163f StPO sobre vigilancia prolongada, que exige autorización judicial. En España, en cambio, hay que distinguir: la circulación o entrega vigilada de bienes asociados a un catálogo de delitos se encuentra regulada en el art. 263 bis LECr, pudiendo autorizarla tanto el juez de instrucción o el Ministerio Fiscal, como los jefes de las unidades orgánicas de policía judicial, centrales o de ámbito provincial, y sus mandos superiores. Por su parte, la acción de agentes encubiertos está regulada en el art. 282 bis LECr y supone en concreto la investigación de actividades propias de la delincuencia organizada, es decir, según la definición legal para estos efectos, "la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer" alguno o algunos de los delitos taxativamente listados (art. 282 bis 4 e] LECr); superada esta restricción, la acción de los agentes encubiertos está supeditada a la autorización del juez de instrucción o, dando cuenta inmediata al juez, del Ministerio Fiscal[32], aunque debe tenerse en cuenta que en el sistema español el juez de instrucción es el responsable de la investigación, con lo cual la diferencia no parece tan significativa.

La diferencia con las regulaciones previas en Chile, básicamente con la matriz del art. 25 de la Ley Nº 20.000, radica fundamentalmente en el involucramiento directo del Fiscal Regional del Ministerio Público, quien debe autorizar las medidas y carga con la responsabilidad por el uso de ellas, debiendo asegurarse de que ella "se limite a las acciones estrictamente necesarias para los objetivos de la investigación, que los agentes reveladores o infiltrados no induzcan

[32] Una visión de conjunto puede verse en Calaza López, Sonia. "Lecciones 14 y 16", en Gimeno Sendra, V.; Díaz Martínez, M.; Calaza López, S. *Derecho Procesal Penal*. Valencia: Tirant lo Blanch (2021), pp. 267 y ss.

a la perpetración de delitos, y que la seguridad de los agentes reveladores o infiltrados se encuentra debidamente resguardada" (arts. 226 B y 226 F). La definición de las técnicas es básicamente la misma existente desde 2005, solo que con mayor desarrollo de detalle.

En lo que concierne a la *exención de responsabilidad penal* de los agentes encubiertos, agentes reveladores e informantes, así como de los funcionarios que intervengan en una entrega vigilada, la norma del art. 226 H es menos precisa que la del art. 25 de la Ley Nº 20.000, que exige no solo que hayan debido incurrir en el delito o que no hubieran podido impedirlo, sino, además, que esto haya sido "consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma", mientras que la nueva regla general se limita a exigir que lo uno o lo otro haya tenido lugar "en cumplimiento de la resolución que autoriza la medida". Como es obvio, no hay resolución de autorización que pueda justificar un homicidio u otro delito grave contra bienes jurídicos personalísimos, por importante que sea la investigación, y no hay razones para pensar que los tribunales lo vean distinto, pero es sin duda más clara y preferible la formulación de la norma en la ley especial.

Para concluir con esta parte, deben destacarse dos disposiciones relevantes desde la perspectiva de la legitimidad de los resultados de la aplicación de las técnicas especiales. Por un lado la prohibición de inducción del art. 226 I y, por la otra, la regulación de las consecuencias de la extralimitación de atribuciones en el art. 226 K.

El defecto central del primer precepto, al margen de su redacción gramaticalmente defectuosa (define inducción por referencia a un resultado consistente en que se cometan delitos que, "de otro modo no habrían sido cometidos", pero específicamente por parte de un sujeto, un "éste", que no ha sido mencionado antes), es que no señala directamente y con la claridad necesaria, atendida la trascendencia del asunto, ninguna consecuencia para la infracción de la prohibición. Bien podría entenderse que, además de la responsabilidad penal por el delito inducido que debiera caberle al inductor (art. 15 Nº 2 CP, no justificado por el art. 226 H, precisamente por la infracción del art. 226 I), corresponde la *exclusión de la prueba* sobre la ejecución del hecho inducido (el testimonio del agente y de terceros, basados en algo que ocurre gracias a la infracción de ley que vulnera derechos del inducido, por ejemplo), conforme al inciso tercero del art. 226 K, por tratarse de un caso manifiesto de inobservancia de los límites no ya solo de la autorización, sino de una prohibición legal expresa. Con todo, esto no es evidente; habría sido exigible que la ley fuera más clara al respecto.

Porque puede haber razonable acuerdo (así puede entenderse también el malogrado intento de redacción del legislador) respecto de que no constituye inducción llevar a cometer el delito a quien está dispuesto de antemano a

cometerlo (*omnimodo facturus*), de modo que se excluye la simple activación de la clara predisposición delictiva del sujeto, expresada en elementos verificables[33], pero sin duda no habrá acuerdo sobre las consecuencias de la efectiva inducción, al menos respecto de la situación del inducido. Si el legislador se iba a dar el trabajo de hacerse cargo del *agent provocateur*, era de esperar que definiera consecuencias. En el derecho comparado, como se sabe, se ha tendido, con mayor o menor fuerza, a reconocer la atenuación o hasta la exención de la responsabilidad penal del sujeto inducido. Así, por ejemplo, en los Estados Unidos se reconoce judicialmente, tanto a nivel federal como estadual, la defensa de *entrapment* que puede conducir a la exoneración del inducido[34]. En el caso alemán, la jurisprudencia ha sido más bien cambiante, pero hay buenas razones para estimar que se ha impuesto una solución equivalente a la estadounidense. En efecto, el Tribunal Supremo Federal consideró durante un tiempo la caducidad de la pretensión punitiva del Estado en casos de una presión significativa sobre ciudadanos sin antecedentes delictivos previos, si bien cambió de rumbo a mediados de la década de 1980, a partir de lo cual, en general, solo se consideraba una posible atenuación[35]; con todo, por influencia de la jurisprudencia del Tribunal Europeo de Derechos Humanos[36], volvió a reconocer una solución que da impunidad al provocado por la vía de un obstáculo procesal[37].

En la medida en que se trata de verdadera inducción estatal, aquí se ve con mucha simpatía esta última solución, y una solución vía exclusión de prueba en virtud del art. 226 K no es despreciable, pero aquí no es posible emitir un juicio fundado definitivo al respecto[38].

---

33 Así, en la discusión estadounidense, Dressler, Joshua. *Understanding Criminal Procedure*, Newark - San Francisco: LexisNexis (2002), p. 580; para Chile, Politoff, Sergio. "El agente encubierto y el informante 'infiltrado' en el marco de la Ley Nº 19.366 sobre tráfico ilícito de estupefacientes y sustancias sicotrópicas", en Politoff, S.; Matus, J.P. (coords.). *Tratamiento penal del tráfico ilícito de estupefacientes*. Santiago: ConoSur (1998), pp. 60-77. Creo que el pasaje del inciso tercero del art. 12 de la Ley Nº 21.459, sobre delitos informáticos, que reza: "No obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos", debe interpretarse como una aclaración de lo que no es inducción, en caso alguno como una excepción a la prohibición de inducción.

34 Dressler, ob. cit., p. 579.

35 El giro se da con BGHSt 33, 356; sobre esto, Roxin, Claus; Schünemann, Bernd. *Strafverfahrensrecht*. München: Beck (2012), p. 306.

36 Furcht v. Alemania, de 23 de octubre de 2014.

37 BGH NStZ 2016, 52.

38 Una visión crítica de la situación en Chile, que justificaba una decisión legislativa más clara, entre otros, en Riquelme, Eduardo. "El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo", en *Polítca Criminal*, Vol. 1, Nº 2 (2006), A2, *passim*;

El segundo precepto sí menciona consecuencias. Si bien la ley no hace distinciones y todo indica que se refiere también a las medidas intrusivas tecnológicas, aquí se considera exclusivamente aquello que dice relación con entregas vigiladas, agentes encubiertos, agentes reveladores e informantes, porque respecto de las primeras la cuestión es clarísima (la prueba obtenida fuera del marco de legitimación que representa la autorización judicial debe ser excluida sin más, de acuerdo con el inciso tercero del art. 276) y no se requieren normas adicionales, máxime si su redacción no es pulcra, como es el caso.

Los dos primeros incisos del art. 226 K caracterizan la extralimitación (por parte del funcionario policial o, respecto de sus órdenes, por parte del fiscal del Ministerio Público), como la inobservancia del "objeto o límites impuestos por la autorización respectiva" o como un "abuso en su ejercicio, en atención a lo autorizado por el Fiscal Regional". Esa definición obliga a considerar el contenido de las autorizaciones de acuerdo con la ley. Así, el inciso sexto del art. 226 B señala que esta debe circunscribir el ámbito de actuación de los agentes en conformidad con los antecedentes y el delito o los delitos invocados en la solicitud, todo esto con el fin de garantizar que se limite a las acciones estrictamente necesarias para los objetivos de la investigación; debe, además, expresar la duración de la autorización (por un máximo de sesenta días, prorrogable por períodos iguales) y establecer las medidas para asegurar los objetivos establecidos[39].

La lectura de estas disposiciones no permite colegir con claridad en qué consiste en concreto la extralimitación, y esto es delicado, porque el precepto, con un lenguaje totalmente ajeno al de la ley procesal penal y que expresa desconocimiento profundo de la lógica de la exclusión probatoria, dispone en su inciso tercero que "el juez de garantía declarará nulas las actuaciones que excedan manifiestamente el objeto de las técnicas especiales y las excluirá, de conformidad con el artículo 276".

No se ve cómo un juez de garantía puede declarar nulas actuaciones policiales (la nulidad procesal, como se sabe, solo se refiere a actuaciones judiciales, art. 159 y ss.) ni que ellas en cuanto tales se excluyan (el art. 276 permite excluir prueba, no actuaciones). Debe entenderse, entonces, que quiere decir que deben excluirse como prueba los antecedentes obtenidos mediante estas técnicas si se ha incurrido en extralimitación. Pero en tal caso, debería aplicarse la lógica

García, Francisco. "Agente revelador, derecho penal del enemigo y fallos de la Corte Suprema", en *93 Revista de la Defensoría Penal Pública*, N° 10 (2014), *passim*.

[39] Respecto de las entradas vigiladas, el inciso cuarto del art. 226 F dispone básicamente lo mismo, debiendo delimitarse "el objeto de la entrega vigilada, así como el tipo y cantidad de las especies de que se trate".

de la inobservancia de garantías fundamentales (subyacente también de algún modo, como se sabe, a la nulidad procesal[40]), y la cuestión es qué de lo que tan vagamente se ha calificado como extralimitación puede considerarse una afectación de las garantías fundamentales de alguien y no simple desobediencia a quien dio la autorización (lo que no justifica ninguna exclusión). Me temo que esto solo se podrá resolver caso a caso.

La regla del art. 226 L se analiza infra IV.

IV. Cuestión transversal: hallazgos casuales

Normativa aplicable

Art. 226 L. *Utilización de medios de prueba.* Los antecedentes o evidencia obtenidos mediante la aplicación de las facultades previstas en este Párrafo y que resulten irrelevantes para el procedimiento serán entregados o devueltos en su oportunidad a las personas respecto de quienes se solicitó la medida y se destruirá todo registro, transcripción o copia de ellos por el Ministerio Público.

Lo prescrito en el inciso precedente no regirá respecto de aquellos antecedentes o evidencia que puedan ser útiles o relevantes para otros procedimientos seguidos por hechos en cuya investigación también sean aplicables las disposiciones de este Párrafo, delitos que merezcan pena de crimen o sean propias del sistema de análisis criminal y focos investigativos, de acuerdo con lo dispuesto en el artículo 37 bis de la ley Nº 19.640.

Art. 226 W. *Hallazgo casual con ocasión de diligencias especiales de investigación.* Si con motivo de las diligencias especiales de investigación previstas en este Párrafo, y en el marco de la autorización concedida por el juez para su ejecución, ocurren hallazgos de objetos, documentos o antecedentes de los cuales no se tenía noticia, que permiten sospechar la existencia de un hecho punible distinto, dichos objetos, documentos o antecedentes podrán ser utilizados para la posterior persecución del delito descubierto, si éste tiene asignado una pena igual o superior a presidio menor en su grado máximo o una pena igual o superior a la del delito objeto de la investigación.

Lo señalado en el inciso anterior no se aplicará a la interceptación de comunicaciones, las que se regirán por lo indicado en el inciso final del artículo 223.

[40] Hernández, Héctor. "La exclusión de la prueba ilícita en el nuevo proceso penal chileno", en *Colección de Investigaciones Jurídicas* Nº 2, Universidad Alberto Hurtado, Santiago (2002), p. 48 ss.

Aunque parecen corresponder a dos situaciones diferentes, el inciso segundo del art. 226 L y el art. 226 W regulan, en rigor, la misma situación. En efecto, si el "hallazgo casual" se puede definir como el descubrimiento de un antecedente no buscado e impertinente para el procedimiento en cuyo marco se dispuso la medida gracias a la cual se obtuvo, pero pertinente para otro procedimiento, y la regla al respecto responde la pregunta de si el antecedente puede aprovecharse en ese otro procedimiento, entonces ambas reglas son, manifiestamente, reglas sobre hallazgo casual. Se podría intentar una distinción a partir de la redacción específica de cada regla, sugiriendo, por ejemplo, que el inciso segundo del art. 226 L supone que el antecedente en cuestión sea pertinente para un procedimiento ya *en curso*, mientras que el art. 226 W se refiere solo a casos en los que se descubre un delito del que no se tenía noticia, iniciándose un procedimiento penal *nuevo*. Pero si eso fuera cierto, en los casos normales de hallazgo casual en el contexto de entradas y registros de lugares cerrados, regidos por el art. 215[41], del cual se tomó inequívocamente la redacción del art. 226 W, los objetos hallados casualmente no podrían servir como prueba en procedimientos ya iniciados por otros delitos, algo que, por cierto, nunca nadie ha sostenido, porque sería sencillamente ridículo[42].

La duplicidad de normas se debe simplemente a que no se vio la peculiaridad del hallazgo casual en el contexto de medidas que, a diferencia de la entrada y registro en lugar cerrado, no están disponibles para la investigación de cualquier delito. En este contexto específico, la cuestión no es si los antecedentes se pueden aprovechar en otros procedimientos, algo que se admite en general, sino *en qué* procedimientos, en particular, por *qué delitos*, siendo la respuesta tradicional (y correcta, desde un punto de vista de proporcionalidad), que solo en procedimientos por delitos cuya investigación hubiera permitido la medida en que se obtuvo el antecedente en cuestión. Por eso, la regla al respecto, la del inciso quinto y final del art. 223, sobre interceptaciones de comunicaciones, aplicable también respecto del art. 226, no está construida al modo del art. 215, sino como una regla que hace excepción al destino que en general deben tener los antecedentes obtenidos gracias a esas medidas extraordinarias. Así, luego

[41] Conviene recordarlo: "*Objetos y documentos no relacionados con el hecho investigado.* Si durante la práctica de la diligencia de registro se descubriere objetos o documentos que permitieren sospechar la existencia de un hecho punible distinto del que constituyere la materia del procedimiento en que la orden respectiva se hubiere librado, podrán proceder a su incautación, debiendo dar aviso de inmediato al fiscal, quien los conservará".

[42] Tan evidente es que ambas normas regulan lo mismo, que el propio art. 226 W, presentado explícitamente como regla de "hallazgo casual", dispone en su inciso segundo que cede ante la norma de aprovechamiento de antecedentes del inciso final del art. 223, del cual el inciso segundo del art. 226 L no es más que una variante.

de haberse ordenado en el inciso anterior que los antecedentes impertinentes o irrelevantes sean entregados a los afectados y sus transcripciones y copias destruidas, este inciso dispone:

> "Lo prescrito en el inciso precedente no regirá respecto de aquellas grabaciones que contengan informaciones relevantes para otros procedimientos seguidos por hechos que puedan constituir un delito al que la ley le asigne pena de crimen, de las cuales se podrá hacer uso conforme a las normas precedentes".

Como se ve, este es el modelo del inciso segundo del art. 226 L[43] y debiera haber sido la norma al respecto, sobre todo en su formulación original, que era impecable, conforme a la cual los antecedentes impertinentes o irrelevantes para la investigación en que se habían obtenido gracias a medidas extraordinarias previstas en el mencionado Párrafo 3º bis del Título I del Libro II, solo podían aprovecharse en investigaciones "por hechos en cuya investigación fueren también aplicables las disposiciones de este Párrafo". Es cierto que los agregados posteriores en el Senado (referencia a crímenes y a delitos objeto del sistema de análisis criminal y focos investigativos) le quitaron consistencia, pero al menos podría decirse que se trata de casos calificados que de algún modo justifican la equiparación. El verdadero problema se produjo con la introducción de una segunda norma sobre lo mismo, el art. 226 W, y con *una solución diferente* (¡). En efecto, mientras el inciso segundo del art. 226 L dispone, como se acaba de decir, que los antecedentes se pueden aprovechar en otros procedimientos "seguidos por hechos en cuya investigación también sean aplicables las disposiciones de este Párrafo, delitos que merezcan pena de crimen o sean [sic] propias del sistema de análisis criminal y focos investigativos"[44], el art. 226 W lo hace posible en investigaciones por delitos que tengan asignada "una pena igual o superior a presidio menor en su grado máximo o una pena igual o superior a la del delito objeto de la investigación"[45].

---

[43] También del inciso noveno del ya mencionado art. 218 ter, sobre datos de tráfico ("Los registros sólo podrán ser utilizados para los efectos de la investigación en la que fueron solicitados, u otras seguidas por delitos que merezcan pena de crimen o sean propias del sistema de análisis criminal y focos investigativos, de acuerdo con lo establecido en el artículo 37 bis de la ley Nº 19.640, que establece la ley orgánica constitucional del Ministerio Público, y no podrán ser utilizados para otros fines"), norma que, sin embargo, tiene poca justificación, porque la medida misma no está sometida a un régimen extraordinario de legitimación, de modo que no se aprecia la razón para que tenga un régimen de hallazgo casual que se aparte del modelo básico del art. 215.

[44] De acuerdo con lo dispuesto en el artículo 37 bis de la Ley Nº 19.640, Orgánica Constitucional del Ministerio Público.

[45] Ambos artículos tienen su origen en sendas indicaciones al proyecto en primer trámite constitucional: el primero en una indicación del Ejecutivo, Informe de Comisión de Seguridad

Esta segunda norma, sobre todo su segundo supuesto de aplicación, representa un grave error legislativo, porque lo único que puede justificar la aplicación de técnicas o medidas extraordinarias para investigar delitos leves, con penas bajas o muy bajas, es su inserción en un contexto de criminalidad organizada o equivalente, de modo que, cuando ese contexto no se da, es absurdo "compensarlo" con una pena al mismo nivel. Como se ha dicho, aunque inconsistente en su formulación final, la fórmula del art. 226 L es sin duda preferible.

El problema es que ambas normas están vigentes y no se aprecia que haya un argumento decisivo para preferir la aplicación del art. 226 L, en tanto que una posible declaración de inaplicabilidad por inconstitucionalidad, con base en el principio de proporcionalidad, argumentando que la afectación de derechos en muchos casos concretos no reconocerá límites mínimos ni contrapesos, no resuelve los problemas inmediatos.

Asumiendo que la práctica se decantara por la norma menos exigente del art. 226 W, el problema no se da tanto en relación con antecedentes obtenidos en el contexto de entregas vigiladas o de actuación de agentes encubiertos, agentes reveladores o informantes, de acuerdo con el nuevo estatuto, en la medida en que estas técnicas no exigen autorización judicial y hasta puede discutirse que, en sí mismas, representen una afectación de derechos fundamentales. Lo realmente grave dice relación con las interceptaciones de comunicaciones y otras formas de captación y grabación de imágenes o sonidos cuando no se dan los requisitos de los arts. 222 y 226, y solo resultan aplicables por el factor organizativo del art. 226 A, en la medida en que el art. 226 W permitiría, por ejemplo, que se aprovechara para la investigación de unas lesiones menos graves, cometidas por quien no tiene ninguna vinculación con el crimen organizado, las grabaciones de una conversación telefónica suya con un sujeto vinculado con una banda dedicada al hurto de supermercados, en la medida que las lesiones menos graves tienen igual o mayor pena que la mayoría de los hurtos que se pueden cometer en un supermercado. Si una regla así rigiera fuera del ámbito del nuevo estatuto, donde las interceptaciones en principio solo proceden tratándose de la investigación de crímenes, esas interceptaciones servirían para probar prácticamente cualquier delito, por insignificante que fuera, es decir, un exceso grosero.

Afortunadamente, la regla del art. 226 W no es aplicable respecto de los arts. 222 y 226, tampoco respecto de normas en otros cuerpos legales, porque

Ciudadana de la Cámara de Diputados, de 5 de mayo de 2021, HL Nº 21.577, p. 135 s.; el segundo en una indicación de los diputados Fuenzalida, Pardo y Torrealba, mismo informe, HL Nº 21.577, p. 143 s. No hay constancia de las razones detrás de ninguna de ellas, y al parecer nadie reparó en el problema que representaba su existencia simultánea.

solo rige para medidas dispuestas en el marco del nuevo estatuto (más que por la afirmación de su inciso final).

V. En particular, medidas de protección de agentes encubiertos, agentes reveladores, informantes y testigos protegidos, en cuanto inciden en las facultades de la defensa

Normativa aplicable

V. De las medidas de protección para agentes encubiertos, reveladores e informantes

Art. 226 N. *Medidas especiales de protección.* Sin perjuicio de las reglas generales sobre protección a los testigos contempladas en este Código, en cualquier etapa del procedimiento el Ministerio Público dispondrá, de oficio o a petición de parte, las medidas especiales de protección que resulten adecuadas cuando estime, por las circunstancias del caso, que existe riesgo o peligro grave para la vida o la integridad física de un informante, agente encubierto, agente revelador o de un testigo protegido, como asimismo de su cónyuge, conviviente civil, ascendientes, descendientes, hermanos u otras personas a quienes se hallen ligados por relaciones de afecto.

Para proteger la identidad, domicilio, profesión y lugar de trabajo de los sujetos indicados en el inciso anterior, el fiscal podrá aplicar medidas tales como:

a) Que en los registros de las diligencias que se practiquen no consten su nombre, apellidos, profesión u oficio, domicilio, lugar de trabajo, ni cualquier otro dato que pueda servir para su identificación. Podrá utilizar una clave u otro mecanismo de verificación para esos efectos.

b) Que su domicilio, para efectos de notificaciones y citaciones, sea fijado en la sede de la fiscalía o del tribunal. El órgano interviniente deberá hacerlas llegar reservadamente a su destinatario.

c) Que las diligencias que tengan lugar durante el curso de la investigación a las que deba comparecer como testigo, se realicen en un lugar distinto de aquél donde funciona la fiscalía y de cuya ubicación no se dejará constancia en el registro respectivo.

Art. 226 O. *Prohibición de revelación de información.* Dispuesta la medida de protección de la identidad a que se refiere el artículo anterior, el tribunal, sin audiencia de los intervinientes, deberá decretar la prohibición de revelar, en cualquier forma, la identidad de los sujetos protegidos o los antecedentes que conduzcan a su identificación. Asimismo, deberá decretar la prohibición para que sean fotografiados, o se capte su imagen a través de cualquier otro medio.

La infracción de estas prohibiciones será sancionada con la pena de reclusión menor en su grado medio a máximo, tratándose de quien proporcione la in-

formación. En caso de que la información fuere difundida por algún medio de comunicación social, se impondrá, además, a su director una multa de diez a cincuenta unidades tributarias mensuales.

En ningún caso el tribunal podrá fundar la condena únicamente en declaraciones realizadas por agentes encubiertos, agentes reveladores e informantes, respecto de los cuales se haya decretado la prohibición de revelación de su identidad.

Art. 226 P. *Declaración en juicio.* Las declaraciones de los agentes encubiertos, agentes reveladores o de testigos y peritos a los que se les otorgue la calidad de informantes podrán ser recibidas anticipadamente en conformidad con el artículo 191 cuando se estime necesario para su seguridad personal. En este caso, el juez de garantía podrá disponer que los testimonios de estas personas se presten por cualquier medio idóneo que impida su identificación física normal. Igual sistema de declaración protegida podrá disponerse por el tribunal de juicio oral en lo penal, en su caso.

Sea que la declaración se preste de manera anticipada o en el desarrollo del juicio oral propiamente tal, el tribunal deberá comprobar en forma previa la identidad del testigo protegido, agente encubierto o revelador o del informante, en particular los antecedentes relativos a sus nombres y apellidos, edad, lugar de nacimiento, estado civil, profesión, industria o empleo y residencia o domicilio. Consignada en el registro tal comprobación, el tribunal podrá resolver que se excluya del debate cualquier referencia a la identidad que pueda poner en peligro su protección.

En ningún caso las declaraciones de los testigos protegidos, agentes encubiertos o reveladores o de los informantes podrán ser recibidas e introducidas en el juicio sin que la defensa haya podido ejercer su derecho a contrainterrogarlo personalmente, con los resguardos contemplados en los incisos precedentes. Si la declaración se presta de forma anticipada, el juez de garantía podrá disponer el alzamiento del secreto establecido en el artículo 226 J y procurará el acceso de la defensa a todos los medios de prueba pertinentes. Sólo lo restringirá en aquellos casos establecidos en el artículo 226 B, inciso final.

Dispuesta por el fiscal la protección de la identidad de los testigos o peritos en la etapa de investigación, el tribunal deberá mantenerla, sin perjuicio de los otros derechos que se confieren a los demás intervinientes.

Art. 226 Q. *Protección policial.* De oficio o a petición del interesado, durante el desarrollo del juicio o incluso una vez que éste ha finalizado, si las circunstancias de peligro se mantienen el fiscal o el tribunal otorgarán protección policial a quien la necesite, de conformidad con lo prevenido en el artículo 308.

Art. 226 R. *Medidas de protección complementarias.* Las medidas de protección antes descritas podrán ir acompañadas de otras medidas complementarias que se estimen idóneas en función del caso, si fuere necesario.

Art. 226 S. *Cambio de identidad.* El tribunal podrá autorizar a los agentes encubiertos, reveladores e informantes a cambiar de identidad, con posterioridad al juicio, en caso de ser necesario para su seguridad.
La Dirección Nacional del Servicio de Registro Civil e Identificación adoptará todos los resguardos necesarios para asegurar el carácter secreto de estas medidas. Todas las actuaciones judiciales y administrativas a que dé lugar esta medida serán secretas. El funcionario del Estado que viole este sigilo será sancionado con la pena de presidio menor en sus grados medio a máximo.
Quienes hayan sido autorizados para cambiar de identidad sólo podrán usar sus nuevos nombres y apellidos en el futuro. El uso malicioso de su anterior identidad será sancionado con la pena de presidio menor en su grado mínimo.
Art. 226 T. *Violación del secreto de la investigación y de la identidad.* La violación del secreto de la investigación y de la identidad de las personas a que se refieren los artículos precedentes será castigada con presidio menor en su grado máximo e inhabilitación absoluta perpetua para cargos u oficios públicos.
Art. 226 U. *Valoración de la prueba y condena.* El tribunal valorará el testimonio de agentes encubiertos, agentes reveladores e informantes conforme a las reglas de la sana crítica.
En ningún caso el tribunal podrá fundar la condena únicamente en declaraciones realizadas por agentes encubiertos, agentes reveladores, informantes y testigos protegidos respecto de los cuales se haya decretado la prohibición de revelación de su identidad.
Art. 226 V. *Protección de las víctimas.* Es deber del Ministerio Público y de las policías otorgar protección a las víctimas de delitos o de amenazas emanadas de asociaciones delictivas o criminales. El fiscal podrá utilizar o solicitar, según sea el caso, la aplicación de las medidas previstas en este Párrafo, aun cuando la víctima no intervenga como testigo o informante.

Por primera vez, la ley establece con carácter general un estatuto reforzado de protección de personas relacionadas con la investigación de delitos con connotaciones de crimen organizado, recogiendo en la codificación procesal penal, con ajustes menores, disposiciones ya contenidas en las Leyes Nº 20.000 (arts. 30 a 37) y Nº 18.314 (arts. 15 a 21). En rigor, el estudio de estas disposiciones, las que, por lo demás y como se acaba de decir, no difieren mayormente de las que se encuentran en estatutos ya conocidos[46], no forma parte del objeto

[46] El único comentario que cabría hacer al respecto es que se constata cierta desprolijidad en la definición de las personas favorecidas por las medidas de protección que se prevén. Así, ciertas disposiciones aluden exclusivamente a agentes encubiertos, agentes reveladores e informantes y no a testigos o testigos protegidos (por ejemplo, el art. 226 S, sobre cambio de identidad), otras incluyen a los testigos y peritos "a los que se les otorgue la calidad de informantes" (art. 226 P) y no a todos, aunque requieran protección, como sí hace, en cam-

de este informe. Si, no obstante, se hace mención a ellas, es, exclusivamente, en cuanto pueden tener como efecto colateral no buscado restricciones de los derechos de la defensa.

Como es obvio, se trata de la protección prestada a través de restricciones de acceso a información que puede ser relevante para preparar la defensa, para impugnar la credibilidad de testigos, para contrainterrogarlos con propiedad, etc. El caso paradigmático es aquel en que se oculta la identidad del testigo (cualquiera sea su calidad adicional) y esto rige también para la defensa, pues es evidente que las tareas recién mencionadas no se pueden realizar competentemente si no se sabe quién es el testigo. Las disposiciones que lo permiten en el nuevo estatuto se encuentran en los arts. 226 N, 226 O y 226 P.

Pues bien, al respecto hay que recordar que el Estado de Chile fue condenado por la Corte Interamericana de Derechos Humanos en el caso *Norín Catrimán y otros vs. Chile*, sentencia de 29 de mayo de 2014, por haber violado, entre otros, el derecho a contrainterrogar a los testigos, consagrado en el art. 8.2 letra f) del Pacto de San José de Costa Rica, por la aplicación de normas que impedían el conocimiento de la identidad del testigo (§ 260 de la sentencia), específicamente en el art. 18 de la Ley Nº 18.314, sobre conductas terroristas, del todo equivalentes a las del nuevo art. 226 P.

La Corte Interamericana entiende que este tipo de medidas puede ser compatible con el Pacto, a condición de que se atienda adecuadamente a ciertos criterios de legitimidad (§§ 245 a 247), cuyos alcances se precisan a propósito del examen del caso concreto (§§ 248 a 252)[47], los que tendrían que estar consagrados en la ley. En concreto, la Corte estableció que el Estado de Chile debía "regular con claridad y seguridad la medida procesal de protección de testigos relativa a la reserva de identidad, asegurando que se trate de una medida excepcional, sujeta a control judicial en base a los principios de necesidad y proporcionalidad, y que ese medio de prueba no sea utilizado en grado decisivo para fundar una condena, así como regular las correspondientes medidas de contrapeso" (§ 436 y disposición Nº 20). Corresponde, en consecuencia, revisar si las disposiciones recién mencionadas satisfacen los criterios sentados por la Corte.

bio, correctamente, el art. 226 N. Puede tratarse de un asunto meramente formal, pero que conviene corregir, porque las consecuencias de una interpretación apegada al texto pueden ser muy graves.

[47] Es el examen del enjuiciamiento de los imputados NC y PP. No es aprovechable, en cambio, en general, el examen respecto del imputado AL, por haberse llevado el proceso en su contra de acuerdo con las normas del Código de Procedimiento Penal de 1906, con sus conocidos déficit.

Básicamente, la reserva de identidad debe adoptarse, primero, bajo un efectivo *control judicial*, con observancia de los principios de necesidad y proporcionalidad (debe tratarse de una medida excepcional, justificada, en concreto, por una efectiva situación de riesgo del testigo); segundo, la afectación del derecho a defensa inherente a la medida debe ser contrarrestada por medidas de contrapeso, tales como el conocimiento de la identidad del testigo por parte del tribunal y acceso directo de este al interrogatorio, de modo de poder observar al testigo y formarse una impresión sobre su confiabilidad, así como una amplia oportunidad concedida a la defensa para contrainterrogarlo directamente; y tercero, la condena no puede estar fundada únicamente o en grado decisivo en declaraciones de este tipo de testigos.

Curiosamente, lo primero, que debería ser lo más fácil de satisfacer por tratarse de medidas que requieren una decisión judicial, parece ser lo más débil en Chile. En el fallo, la Corte constató un control judicial insuficiente, pues la resolución judicial que dispuso la reserva de identidad no contenía una motivación explícita, limitándose a hacer lugar a la solicitud del Ministerio Público que, por su parte, solo invocaba genéricamente la "naturaleza", las "características", "circunstancias" y "gravedad" del caso, pero sin especificar aquello que, en el caso concreto, fundara el riesgo que se alegaba para los testigos y su entorno (§ 249). Y lo cierto es que la ley no orienta mayormente al tribunal, a pesar de que, en rigor, es un deber esencial del cargo. En efecto, el art. 226 O sugiere que el juez simplemente debe darle respaldo a la medida de protección dispuesta por el Ministerio Público, sin exigencia (ni posibilidad, al menos no explícita) de ponderación ("deberá decretar" las prohibiciones allí previstas).

A la hora de buscar una solución, es posible que un malentendido, en el que puede haber caído también la Corte Interamericana, esté complicando aún más las cosas. No es razonable (y puede ser gravísimo) que, a menos que se haya disipado completa y ostensiblemente cualquier riesgo para el testigo o su entorno, un tribunal le quite respaldo a una medida de protección dispuesta por el Ministerio Público, menos aún a resoluciones judiciales previas que les dieron respaldo. Lo que, en rigor, debe controlar el juez es si se justifica que las personas beneficiadas por esa medida puedan servir como prueba en el proceso, a pesar de que, con ello, se merman las posibilidades de ejercicio del derecho a defensa. Para ello, el tribunal debe arribar a la convicción (y fundarlo debidamente) de que, por una parte, la revelación de la identidad del testigo acarrea un peligro real, concreto y atendible, para él o para su entorno, y que, por la otra, su deposición como testigo es, sin embargo, necesaria. Si no es el caso, los jueces de garantía debieran imponerle al Ministerio Público la decisión, en el sentido de optar entre protección o testimonio, a través del mecanismo

previsto en el art. 10, pero nunca levantar la protección del testigo[48]. En el caso del tribunal del juicio, debería abstenerse explícitamente de valorar el testimonio[49], solución que, si bien puede confundirse con el tercer punto, es decir, con la cuestión concerniente al peso del medio de prueba en la sentencia, destaca el aspecto de control judicial exigido por la Corte Interamericana. En espera de un reforzamiento legal de dicho control judicial, que sería deseable desde un punto de vista de convencionalidad, un comportamiento judicial como el sugerido podría servir como nota de legitimidad del derecho chileno en la materia. Desde el punto de vista de la defensa, de la mano de la sentencia interamericana, este debería ser objeto predilecto de revisión y posible impugnación vía recurso de nulidad.

Respecto de lo segundo (medidas de contrapeso), la ley parece satisfacer las exigencias de la Corte (debe recordarse, por lo demás, que esto se reconoció ya en el caso concreto, con el simple cumplimiento de las normas legales, § 250), pues, de acuerdo con el inciso segundo del art. 226 P, el tribunal debe comprobar previamente la identidad del testigo, "en particular los antecedentes relativos a sus nombres y apellidos, edad, lugar de nacimiento, estado civil, profesión, industria o empleo y residencia o domicilio", mientras que el inciso tercero dispone que "[e]n ningún caso las declaraciones de los testigos... podrán ser recibidas e introducidas en el juicio sin que la defensa haya podido ejercer su derecho a contrainterrogarlo personalmente"[50].

Y respecto de lo tercero (evitación de efecto determinante en la sentencia), se ha incluido una regla de valoración de prueba que, a todas luces, está tomada del fallo, a saber, el art. 226 U, cuyo inciso segundo dispone lo siguiente:

---

[48] Sin perjuicio de que una condena basada en testimonios que no satisfacen este escrutinio debería poder ser anulada conforme a la letra a) del art. 373, no parece que se den los requisitos del inciso tercero del art. 276 para excluir al testigo como prueba, porque lo que vulnera garantías en este caso no es la obtención de la prueba, sino su incorporación *en juicio* de un modo que impide a la defensa, injustificadamente, ejercer sus derechos.

[49] Porque en este caso, las condiciones concretas de la incorporación de la prueba en juicio hacen de ella "prueba ilícita". A pesar de ser un asunto controvertido, la no valoración de prueba ilícita (conocida también como "valoración negativa") parece haberse asentado en la práctica judicial chilena. Una visión completa y actual del asunto puede verse en Correa, Carlos. "La llamada valoración negativa de la prueba en la doctrina y la jurisprudencia", en *Latin American Legal Studies*, Vol. 8 (2021), p. 65 y ss.

[50] Y si se trata de una declaración anticipada, esto es, en un momento en que ciertos antecedentes pueden ser aún secretos para la defensa, conforme al art. 226 J, el tribunal "podrá disponer el alzamiento del secreto establecido en el artículo 226 J y procurará el acceso de la defensa a todos los medios de prueba pertinentes". El carácter facultativo del alzamiento genera dudas sobre la satisfacción del derecho de defensa en este punto específico.

> "En ningún caso el tribunal podrá fundar la condena únicamente en declaraciones realizadas por agentes encubiertos, agentes reveladores, informantes y testigos protegidos respecto de los cuales se haya decretado la prohibición de revelación de su identidad"[51].

Sobre esto último, con todo, debe verificarse el cumplimiento efectivo de lo dispuesto en la regla, al modo en que lo hizo la Corte en el caso concreto. Respecto de uno de los acusados, se concluyó que el testimonio del testigo protegido no había sido decisivo; pero respecto del otro, ese testimonio sí lo habría sido, pues

> "si bien se hace referencia a otros medios de prueba, éstos por sí solos no hubiesen bastado para llegar a la condena, ya que las otras tres personas que rindieron testimonio solo tenían un conocimiento indirecto. La sentencia hizo además referencia a una carta sobre supuestas amenazas firmada por el señor P, pero sin fecha, y a un cheque firmado por el administrador del FN a la orden del acusado" (§ 251).

Este ejercicio debería servir de modelo para fundar un eventual recurso de nulidad de acuerdo con la letra a) del art. 373.

Nota complementaria

Con posterioridad a la entrada en vigor de la Ley Nº 21.577 y de la facción del informe precedente, entró en vigor la Ley Nº 21.694, de 4 de septiembre de 2024, que modificó el art. 226 A del Código Procesal Penal[52] y, con ello, el ámbito de aplicación de las técnicas especiales de investigación previstas en el Párrafo 3º bis del Título I del Libro II de dicho cuerpo legal, introducido el año anterior mediante la mencionada Ley Nº 21.577. El art. 226 A original disponía:

> "Las técnicas especiales de investigación previstas en este Párrafo serán aplicables en la investigación de hechos que involucren la participación en una asociación delictiva o criminal, de acuerdo con lo previsto en los artículos siguientes".

[51] Regla que también se encuentra, incomprensiblemente, en el inciso final del art. 226 O. La regla del inciso primero ("El tribunal valorará el testimonio de agentes encubiertos, agentes reveladores e informantes conforme a las reglas de la sana crítica"), tomada probablemente del § 247 de la sentencia, simplemente denota desconocimiento del legislador (¡) del régimen probatorio que rige en el proceso penal chileno.

[52] De nuevo, en lo sucesivo, artículos sin otra mención corresponden a los de este código.

La nueva ley agregó al supuesto original de aplicación el siguiente:

"o bien cuando se trate de hechos que hagan presumir fundadamente la existencia de alguna de ellas".

El agregado surge de una indicación del diputado Andrés Longton en Segundo Trámite Constitucional, que fue aprobada por mayoría de votos en la Comisión de Constitución, Legislación, Justicia y Reglamento de la Cámara de Diputados[53] y se mantuvo sin alteraciones hasta el despacho de la ley. De los materiales legislativos se desprende que el propósito perseguido era hacer frente al problema que se produce cuando, luego de emplearse las técnicas especiales en la investigación de un hecho particular, se advierte que en la especie no se daban los presupuestos legales para la aplicación de tales técnicas especiales, esto es, en el régimen original, que se tratara de "la investigación de hechos que involucren la participación en una asociación delictiva o criminal". Esta situación, según se ha argumentado en el informe precedente (I.), debería dar lugar a que el material probatorio obtenido gracias al empleo de esas técnicas no pudiera ser valorado en el enjuiciamiento de los hechos respecto de los cuales dicho empleo no era legalmente posible. Con la nueva redacción se habría procurado evitar esa consecuencia.

En efecto, luego de un debate sobre su admisibilidad, el autor de la indicación apuntaba al respecto lo siguiente:

"Es importante que se pueda 'presumir fundadamente' porque se utilizan técnicas especiales de investigación y si, posteriormente, se descubre que no era una organización delictiva, en una revisión ex post del tribunal, se puede objetar desde el punto de vista de cómo se ha llevado a cabo la investigación, se puede producir un problema con la prueba y puede ser perjudicial para el objetivo que se quiere lograr respecto a la condena de quien comete delitos graves"[54].

Con lo cual, al parecer, entendía estar excluyendo un escrutinio *ex post* sobre la efectiva procedencia del empleo de las técnicas especiales de investigación. Sin perjuicio de que en la intervención transcrita no se expresan razones en favor de semejante solución, no parece ser que la indicación logre ese propósito. Porque ya en la escueta discusión que esta generó en la comisión, al menos quedó meridianamente claro que la procedencia de la técnica especial en un caso concreto no se resolvía de modo definitivo al momento de resolverse su

[53] Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento de la Cámara de Diputados, de 10 de enero de 2024, Biblioteca del Congreso Nacional, Historia de la Ley Nº 21.694 (en lo sucesivo, HL Nº 21.694), pp. 578-581.

[54] HL Nº 21.694, p. 579.

aplicación, sino que puede y debe ser objeto de revisión posterior. Así, por ejemplo, se desprende de la intervención del abogado de la División Jurídica del Ministerio de Justicia, quien

> "señala que habiendo revisado la indicación - que conoció ahora - lo que resulta de la aplicación de este criterio no resuelve el problema del análisis ex post, si el fiscal se equivocó o no al ocupar la técnica de investigación que no estaba frente a una organización criminal, eso hay que tenerlo claro. La indicación establece un criterio sobre el cual el fiscal debiese decidir, si esa es la intención, lo que hace en realidad la norma propuesta es ponerle una carga al fiscal de fundamentación al momento de decidir utilizar un mecanismo especial de investigación de los artículos 226 y siguientes, por lo tanto, le va a dar un criterio más o menos objetivable al juez de garantía para excluir la pena. Si eso es así, está de acuerdo con la norma"[55].

Y tanto o más importante, así lo reconoce también el representante del Ministerio Público en la discusión, el abogado Ignacio Castillo, cuando afirma:

> "En este caso el fiscal regional[56] va a tener que establecer presunciones fundadas - comparte que va a obligar a fundamentar mejor por qué se tomó tal decisión en un estado incipiente, por ejemplo, porque había antecedentes, porque no se tenía la identidad pero se sabía que era una banda dedicada a la extorsión. Por lo tanto, al momento de la exclusión de prueba, se va a fundamentar que había presunciones fundadas. Siempre va a existir la posibilidad que algún juez considere que no las había.
>
> El legislador le está dando una buena señal al juez de que tiene que haber una presunción fundada, y esa va a tener que estar motivada y fundamentada por el fiscal regional; lo que va a permitir que, a pesar de que no esté completamente conformada la asociación criminal, se puedan usar las técnicas de investigación. Le parece una buena indicación"[57].

Lo que es confirmado finalmente por el diputado Raúl Leiva, quien presidía a la sazón la comisión, cuando, al tomar la palabra en este contexto específico,

> "señala que siempre existirá una oportunidad para discutir y excluir una prueba"[58].

---

55 HL Nº 21.694, p. 579.

56 La referencia a la decisión del fiscal regional del Ministerio Público solo es pertinente respecto de la intervención de agentes encubiertos y figuras análogas, pero es manifiesto que el razonamiento es de alcance general.

57 HL Nº 21.694, p. 580.

58 HL Nº 21.694, p. 580.

Consecuentemente, lo único que puede estar en discusión es el *alcance* del necesario examen *ex post* sobre la procedencia de los presupuestos legales de la aplicación de las técnicas especiales en el caso concreto. Una lectura posible sería entenderlo como un examen de la corrección o suficiencia del juicio *ex ante* en virtud del cual se autorizó judicialmente (o por parte del fiscal regional, en el caso de los agentes encubiertos y figuras análogas) la técnica extraordinaria de investigación, esto es, nada distinto de lo que procede en un examen sobre la legitimidad de la obtención de la prueba para efectos de la posible exclusión de la prueba ilícita. Ocurre, sin embargo, que en este contexto específico, tal como se hizo presente en el informe precedente (I.), no se trata de la legitimidad de la autorización en cuanto tal, que debe establecerse, en efecto, conforme a un juicio *ex ante*, sino que de una cuestión de *proporcionalidad* que es independiente de la rectitud de la actuación de los agentes. Aunque la prueba se haya obtenido de un modo *ex ante* legítimo, la cuestión es si ella puede servir para establecer un hecho respecto de cuyo establecimiento el modo en que fue obtenida estaba legalmente excluido. La lógica del problema no es la de la exclusión de la prueba ilícita, sino que se acerca más a la del aprovechamiento de los hallazgos casuales en el marco de una actividad investigativa sometida a restricciones de proporcionalidad: así, por ejemplo, en el caso de una interceptación telefónica, nadie duda de la legitimidad de tales hallazgos cuando tienen lugar al amparo de una autorización procedente en los términos del art. 222, no obstante lo cual la ley solo permite su aprovechamiento para el establecimiento de hechos en cuya investigación la interceptación hubiera sido posible (art. 223 inciso final). La diferencia radica en que aquí no se trata de un hallazgo casual en el marco de una actividad procedente (razón por la cual no tiene efectos la defectuosa regulación de los hallazgos casuales en los arts. 226 L y 226 W, denunciada en el informe precedente, IV.), sino de lo que se obtiene en el curso de una actividad improcedente.

Ahora bien, no sería una lectura leal de la ley pretender que el cambio legislativo no ha tenido ningún efecto y que, tal como se decía en el informe precedente (I.), deba constar necesariamente, aunque sin necesidad de alcanzar el estándar de la convicción más allá de toda duda razonable, la "tipicidad objetiva" de los tipos penales de los arts. 292 o 293 del Código Penal. Esto, desde luego, porque implicaría afirmar que ambas hipótesis del art. 226 A tienen exactamente el mismo alcance. De ahí que no se pueda exigir un juicio desde una perspectiva estricta *ex post*, que conduciría precisamente a ese resultado. Más bien, de lo que parece tratarse es, por una parte, de un juicio exigente, calificado, sobre la racionalidad *ex ante* de la medida, tal como se indicó en la historia fidedigna del establecimiento de la ley a propósito del concepto de presunción fundada, pero con la diferencia, por la otra, de ser un juicio que abarca no solo la situación al tiempo de la autorización de la medida, sino

que se extiende a lo largo de su ejecución. De este modo, cualquier atisbo de decaimiento del presupuesto legal de procedencia de la medida debe dar lugar inmediatamente a su cese, siendo de responsabilidad exclusiva del Ministerio Público la observancia permanente de este estándar, debiendo soportar, en caso contrario, la imposibilidad de aprovechar la prueba obtenida. Solo así se puede evitar el riesgo involucrado en un control blando del empleo de estos medios extraordinarios, que es que, en los hechos, baste la mera invocación liviana de sus presupuestos legales para disponer de algo que la ley quiere reservar solo para casos excepcionales.