Maximiliano Hairabedián

Investigación y prueba del narcotráfico

Políticas antidrogas - Jurisdicción y competencia
Desfederalización - Despenalización - Drogadependencia
Microtráfico - Proporcionalidad de las penas - Narcotráfico
de mediana o gran escala - Uso de tecnología - Operaciones
encubiertas - Entrega vigilada - Informantes - Arrepentidos
Investigaciones patrimoniales - Lavado de activos - Decomiso
Extinción de dominio - Allanamiento - Requisa - Acceso
a las comunicaciones telefónicas y digitales - Interrupción
y apertura de encomiendas y paquetes Interceptación y derribo
de aeronaves - Drones - Controles preventivos - Actas - Pericias
Cadena de custodia - Nuevo Código Procesal Penal Federal

Con la colaboración de Ignacio Verde

AD-HOC

allá de que la legislación no exige la confesión, lo cierto es que, se autoincrimine o no, declara en causa propia. Y si bien existe controversia en cuanto a si existe un "derecho a mentir" del imputado con rango constitucional y eventualmente sobre sus alcances,[414] la Constitución no establece tal derecho y menos en circunstancias como las apuntadas en la cual no se lo toma como presunción de culpabilidad, por lo que es razonable su tipificación.

para la confesión el Estatuto Provisional de 1815 y expone el comentario de Obarrio en la exposición de motivos del antiguo Código de Procedimiento en materia penal: "…la indagatoria se tomará en la forma que el proyecto determina, sin que jamás pueda hacerse al procesado preguntas capciosas o sugestivas ni emplearse coacciones. amenazas o falsas promesas, ni exigirle juramento ni aún simple promesa de decir la verdad, bajo el concepto de ser corregido disciplinariamente el juez que violara estas prohibiciones legales, si no hubiere lugar de su parte a una responsabilidad mayor". De Luca consigna que "la Corte Suprema adoptó esta posición desde sus comienzos y la mantuvo: *Fallos*, 1:350; 227:63; 281:177" desarrollando el contenido de precedentes al respecto (De Luca: "Notas sobre la cláusula contra la autoincriminación coaccionada", cit., pp. 266/267).

[414] "El imputado en un proceso penal no está sometido a la obligación jurídica de decir la verdad, sino que puede callar total o parcialmente o incluso mentir, en virtud de los derechos a no declarar contra sí mismo y a no confesarse culpable y que no pueden extraerse consecuencias negativas para el acusado derivadas exclusivamente del ejercicio de su derecho a guardar silencio o de los derechos a no declarar contra sí mismo o a no confesarse culpable (TC España, S. nº 76 16/4/2007). El Tribunal Superior de Justicia de Córdoba ha resaltado la conexión entre el principio de inocencia y el derecho de defensa, pues proporciona a este su verdadero sentido, de modo que no se podrá utilizar como presunción de culpabilidad en su contra, ni como circunstancia agravante para la individualización de la pena que se le pudiere imponer, art. 41 C.P., que el imputado se abstenga de declarar, o que al hacerlo mienta, o el modo en que ejerza su defensa (Sent. nº 45, 27/5/2004, "Alfaro"). Cafferata Nores, al cuestionar el uso de la mentira del imputado para perjudicarlo en la valoración de la prueba, aclara que "por cierto que no se pretende aquí abordar toda consecuencia perjudicial que pudiere acarrearle cualquier mentira que pronuncie en ese acto procesal. Por ejemplo, si sus dichos resultan agraviantes para el honor de una persona por imputarle falsamente un delito de acción pública, podrá –eventualmente quedar sujeto a responsabilidad penal o civil (art 109 CP); o si proporciona datos falsos sobre el delito de terrorismo que se le imputa buscando las ventajas del "arrepentido", quedará sujeto a las sanciones expresamente previstas para ese supuesto en el art. 6º de la ley 25241" (¿Es constitucionalmente aceptable el indicio de "mala justificación?". Entre el "vuelo de la golondrina" y el "vuelo del murciélago", Academia de Derecho y Ciencias Sociales, Córdoba, *http://www.acaderc.org.ar/es-constitucionalmente-aceptable-el-indicio-de-mala-justificacion*).

Capítulo VIII
ACCESO A DATOS DIGITALES Y TELÉFONOS CELULARES

"Hoy el gobierno puede escuchar todo lo que digas, sabe dónde estás, con quien hablas, y créeme, sabe con quién te acuestas. Si enciendes un teléfono celular o una computadora estás perdido. Pero en la Colombia de 1989 no era tan fácil. Para empezar, no había internet, ni celulares. Lo máximo eran los teléfonos satelitales, y para captar uno había que volar justo encima. Además, los únicos que tenían uno eran los millonarios, los terratenientes, los políticos. Y por suerte para nosotros, los narcos eran los más ricos de todos".

Presentación del comienzo de la serie *Narcos* que se emite por Netflix.

"La tecnología casi nunca es neutral. Y cada individuo es conocido por el Estado, y todos sus amigos también, y puede ser rastreado con exactitud, como resultado de las comunicaciones. Entonces, cuando el Estado se vuelve malo, los individuos no tienen dónde esconderse".

Julián Assange.

I. *Introducción*

Es notorio el cambio de modelo en la investigación del narcotráfico —y otros delitos— que se operó en los últimos años con la irrupción masiva de los teléfonos celulares e internet. Facilitan la comisión del delito pero también las posibilidades de su descubrimiento. En qué medida y porcentaje se dan estas dos realidades depende de muchos factores, pero los límites técnicos y legales son los principales.

El teléfono móvil se ha convertido en un instrumento contenedor de la vida privada. Son tantas las aplicaciones y usos, que el secreto de las llamadas termina siendo una mínima parte. Los mensajes (*sms, whatsapp, telegram*, correos electrónicos, etc.), las fotografías, videos, audios, localizaciones por GPS, búsquedas por la *web*, intereses, lecturas, archivos, notas, compras, operaciones bancarias, etc., pueden guardar los aspectos más íntimos de la persona. Hace un par de décadas las computadoras comenzaron a compartir espacios de almacenamiento de la intimidad con los lugares tradicionales (escritorios, armarios, bibliotecas, cajas, libretas, álbumes de fotos). Y más recientemente el mismo fenómeno ocurrió con los celulares. Tanta información obviamente constituye un reservorio importante de prueba. De allí el interés en escudriñar los problemas jurídicos que se plantean cuando se pretende registrar un teléfono celular con fines de investigación penal. Porque distinto es el procedimiento para la obtención de evidencia electrónica almacenada por los proveedores de servicios (correos electrónicos, redes sociales, aplicaciones móviles, etc.). En términos generales, en Estados Unidos se clasifica la información según la mayor o menor invasión a la privacidad del usuario, como básica, transaccional y de contenido. La importancia de la clasificación previa radica en que el canal que deba utilizarse dependerá de la información solicitada. La primera puede referirse a datos del titular de la cuenta, teléfonos asociados, correos de recupero, datos de tarjetas de crédito, últimos accesos con indicación de IP. La obtención de esta información está sujeta al estándar de oficio a la empresa mencionando a utilidad y pertenencia, no siendo necesario un exhorto. La segunda (transaccional) abarca datos de remitente y receptor de correos e IP de conexión, sitios visitados. Para ello se requerirá orden del juez con mención de la utilidad y pertinencia y exhorto internacional. En tanto que la información de contenido se refiere al texto, archivos adjuntos, publicaciones cerradas en redes sociales, historial de localización, fotos y documentos. Para el acceso se requiere orden del juez fundada en causa probable y exhorto internacional.[415]

[415] "Guía de obtención, preservación y tratamiento de evidencia digital", elaborada por la Unidad Fiscal Especializada en Ciber-delincuencia (UFECI), a cargo del fiscal Horacio Azzolin, aprobada en el marco de la XVII Reunión Especializada de Ministerios Públicos del Mercosur, celebrada en Buenos Aires, entre el 18 y 20 de noviembre de 2014. Aclara que "más allá del pedido de información (básica, transaccional o de contenido) y de la preservación, en algunos casos las empresas pueden entregar voluntariamente información (de suscriptor, de contenido o ambas) sin necesidad de exhorto. El procedimiento se denomina Emergency Disclosure Request (EDR). A esos efectos, debe demostrarse que existe una emergencia que involucra riesgo inmediato de muerte o de seria afectación a la integridad física de una persona, y que esta situación genera que se entregue la información sin demora. En estos casos el pedido puede realizarse en forma directa a las empresas, las cuales evaluarán si el supuesto planteado amerita apartarse de las reglas generales, para lo cual usualmente solicitan información específica al requirente".

Nos referiremos ahora a medidas de investigación que tienen por objeto un aparato móvil que está en poder del usuario o a disposición de los órganos oficiales (v. gr., el celular secuestrado), dejando de lado la problemática referida a la intervención de comunicaciones, que al igual que la interceptación de correspondencia se caracterizan porque interfieren el proceso mismo de la comunicación, el diálogo o tránsito que se da en el lapso comprendido entre la emisión y la recepción (p. ej., si se quieren conocer los mensajes en el momento en que son enviados).[416]

La problemática del acceso y obtención de datos en teléfonos celulares tiene muchas aristas, pero entre las más importantes se encuentran la determinación de la afectación a la intimidad, los límites y alcances, la selección de las vías legales y los requisitos para su realización. Las medidas de investigación que implican una injerencia en los derechos constitucionales, tienen la regla de la taxatividad legal (CADH, art. 30),[417] por lo que es de suma im-

[416] "No existe intromisión en el derecho al secreto de las comunicaciones (sino intervención en el derecho a la intimidad) en los supuestos de acceso por la policía a una carta abierta que el detenido llevaba consigo en el momento de la detención (STC 70/2002, de 3 de abril); examen por la policía de la pantalla de un teléfono fijo para identificar una llamada entrante o comprobación de la memoria del aparato (STS 3/3/2000); examen de los mensajes SMS registrados en un teléfono móvil intervenido (SSTS 27/6/2002, 30/11/2005); examen del registro de llamadas de un teléfono móvil (SSTS 25/9/2003, 25/7/2003 y 30/11/2005; STC 56/2003, de 24 de marzo)" (TS Español, S. 41, 26/1/2010).

[417] La casación federal tiene dicho que "toda medida de restricción que importa una afectación de los derechos fundamentales, debe ser sometida al test de orden internacional y constitucional que informa la teoría general de los límites o conjunto de requisitos formales y materiales para las restricciones de derechos, que operan a modo de límites a la capacidad limitadora, y que deben ser sorteados; a saber, entre otros: la habilitación constitucional, la reserva de ley, la causalización, la judicialidad, la adecuación, la necesidad, la proporcionalidad y la compatibilidad con el orden democrático" (CFCP, Sala II, reg. nº 1788, 5/11/2015, "Hinricksen", citando el precedente "Díaz", reg. nº 19.518 del 25/11/2011).

portancia establecer en cada caso de acceso a datos de celulares si implican un avance sobre una expectativa legítima de privacidad, y en este caso verificar la existencia de una norma que la autorice. En cambio, en materia probatoria es sabido que rige el principio de la libertad. Por eso es importante no confundir medidas de investigación con medios de prueba. Las primeras solo sirven para generar una hipótesis de investigación o bien como herramienta o medio de adquisición de evidencias.

Cuando hablamos de escarbar en un teléfono con fines probatorios, podemos estar frente a una medida con gran poder de afectación del derecho a la intimidad. Y esto produce inevitablemente la clásica tensión entre el interés estatal y social en probar y penar el delito, y el respeto de los derechos y garantías constitucionales. El constante avance tecnológico genera permanente y rápidamente nuevos y complejos desafíos para la resolución de esa tensión, el derecho suele correr detrás de ese desarrollo, pero cuenta con la base y ventaja de las construcciones constitucionales anteriores.

Maier dice que dentro de la problemática de las exclusiones probatorias, desarrollada históricamente sobre la base de los métodos de investigación tradicionales, aparece hoy agregado un problema nuevo, perteneciente a la llamada 'posmodernidad' y de la mayor gravedad, pues el alcance veloz y, al parecer, arrollador, de las ciencias naturales y de la técnica —frente a los tiempos de las ciencias culturales (una de las cuales es la ciencia jurídica), verdaderas tortugas en comparación con aquellas— ha concebido medios de indagación de la verdad y de información que superan geométricamente las posibilidades antiguas, desde escuchas a distancia con trasmisores supersensibles, trasmisiones audiovisuales o grabaciones ocultas, hasta el cruzamiento de informaciones almacenadas en bancos de datos, posible en tiempo útil solo por ordenadores, considerándolo uno de los temas más complejos y polémicos de la dogmática procesal penal.[418]

Orin Kerr, pone el foco de atención sobre el cambio tecnológico y social como mecanismo del desarrollo del derecho a la intimidad, ilustrando la existencia de un derecho al respecto como un árbol crecido con muchos anillos que han ido formando su tronco. A

[418] Maier, Julio B. J.: *Derecho procesal penal*. t. II, *Parte General,* Editores de Puerto, Buenos Aires, 2003, pp. 134 y ss., citado por Muñoz Conde: "Prueba prohibida y valoración...", cit., p. 99.

medida de que cada anillo se agrega, el árbol va creciendo, y así el derecho de la cuarta enmienda de la constitución norteamericana se erige caso por caso, con cada anillo creciendo en respuesta a alguna nueva tecnología o cambio que se produce. De la misma manera que se puede observar un árbol adulto como un edificio fijo, el derecho de la intimidad puede verse como una masa sólida difícil de explicar. Los estudiosos se enfocan sobre las capas de principios que forman la doctrina, y en ese proceso han visto extraer el significado de la cuarta enmienda desde sus grandes tests, tales como el de la "razonable expectativa de privacidad" y el balanceo de la "razonabilidad".[419] En realidad la metáfora del árbol no es novedosa. Ya a fines de los años 80 Dworkin propuso entender la interpretación constitucional a la luz de una imagen que adquiriría enorme peso: "la novela en cadena" escrita por una diversidad de autores a lo largo del tiempo.[420] Para comprender la "novela en cadena" Gargarella pide que imaginemos que "somos veinte personas que participamos en esta tarea, y que cada uno se compromete a escribir cinco páginas de esa novela. Cada uno, cuando recibe el manuscrito que le lega quien lo antecede en la obra, agrega entonces sus cinco hojas, que pasan a sumarse a las hojas ya escritas por todos sus antecesores. Continúa el constitucionalista diciendo que entonces Dworkin nos pregunta: "¿qué es lo que una persona responsable, comprometida con su tarea,

[419] Concluye que la Corte Suprema de su país continúa intentando mantener el equilibrio de la cuarta enmienda en un mundo cambiante y el ajuste del equilibrio ha provisto la herramienta crítica para lograr ese vital objetivo (Kerr, Orin S.: "An equilibrium-adjustment theory of the fourth amendment", *Harvard Law Review*, vol. 125, pp. 542 y 543). En similar sentido, se ha dicho que una importante cuestión que merece atención antes de dejarla ir es aquella centenaria y antigua de que el policía en la calle no necesita desviar la mirada del delito en público. Fue establecida por la época de Lord Chief Justice Camden cuando escribió en "Entick v. Carrington" que "el ojo, según las leyes de Inglaterra, no puede ser culpable de pecado". Es difícil discutir con esa lógica. Existe una profunda apelación intuitiva a la idea que no podemos pedirles a los policías, quienes prestaron juramento de proteger y servir, que en situaciones de peligro lo pasen por alto. Ahora que estamos perdiendo las restricciones estructurales de la privacidad, a veces la cuarta enmienda podría forzar a la policía a desviar sus ojos hacia los hechos fácilmente perceptibles (Ohm, Paul: "The fourth amendment in a world whitout privacy", *Mississippi Law Journal*, vol. 81:5, p. 1353).

[420] Dworkin, Ronald: *Law's empire*, Harvard University Press, 1988, citado por Gargarella, Roberto: "Interpretar el derecho. Entre la 'novela en cadena' y la 'catedral bombardeada'", *LL*, 27/7/2016, p. 1.

debe hacer, una vez que recibe el manuscrito en cuestión?"; las respuestas son relativamente obvias. La primera obligación de cada participante es leer las páginas ya escritas. Luego, cada uno tratará de entender lo escrito, y de darle un sentido a todo lo escrito. Finalmente, tratará de completar sus cinco páginas, dándole "la mejor continuación posible" a la novela hasta entonces escrita: una continuidad que haga honor a lo ya escrito, y que prepare el camino para el próximo participante. Para Gargarella, este simple ejemplo que nos ofrece Dworkin, tan sencillo e intuitivo como parece, es sin embargo tremendamente revelador acerca de lo que es y lo que debe ser la interpretación constitucional, si es hecha responsablemente. Agrega que después, otros doctrinarios propusieron refinar y precisar aquella imagen, a través de la "catedral," vista de modo completo para ser reconocida y entendida en un sentido pleno (Guido Calabresi inauguró el uso de esta otra metáfora, a través de un famoso artículo publicado en 1972). Luego pasa a dar cuenta de esas tres metáforas. Con una construcción colectiva, consistente en este caso en una Catedral que una comunidad va desarrollando, generación tras generación. Pone el ejemplo de la Iglesia de la Sagrada Familia, en Barcelona, que la comunidad catalana viene erigiendo desde hace más de un siglo, y que aún no ha terminado. Si ellos se propusieran revolucionar la arquitectura contemporánea, con la terminación de este proyecto aún no cerrado, posiblemente equivocarían su objetivo: la misión que tienen asignada no es la de desarrollar la más grandiosa iglesia imaginable, sino una tarea muy diferente, que consiste en concluir una obra que la comunidad ha comenzado por Antonio Gaudí en 1882. Lo mismo en el derecho, y lo mismo para cada juez que se apreste a decidir un nuevo caso. En efecto, si el juez —como el arquitecto— mirase a su pendiente obra, con la certeza de estar en posesión de cualidades extraordinarias, ansioso por ponerlas en práctica, y con desdén hacia lo ya construido, simplemente equivocaría su tarea: su misión es la de continuar una construcción colectiva, y no empezarla de cero, deslumbrando al resto. El autor propone, para pensar sobre la interpretación del derecho en la Argentina —en el marco de sistemas institucionales frágiles, golpeados, imperfectos—, la imagen de una "catedral bombardeada… con paredes por completo deshechas, todos los cristales de las ventanas destruidas, su cúpula descabezada pero, aún así, y a pesar de todo, con sus pilares básicos aún sobre sus pies, con una estructura definida, con ciertas líneas claras que nos permiten

distinguir de qué tipo de obra se trata. Su discontinuidad característica, Cortes que se suceden unas a otras, gobierno a gobierno, cada una con una composición diferente de la anterior; saltos entre tipos y estilos de administración, casi opuestos entre sí, golpes de Estado explica en parte las variaciones drásticas, a veces dramáticas, líneas de jurisprudencia radicalmente cambiantes (i.e., las variaciones que fueron de Bazterrica a Montalvo, y de Montalvo a Arriola, en materia de consumo personal de estupefacientes. Gargarella concluye que necesitamos terminar con el "zigzagueo constante" (donde pasamos de una construcción "clásica" a otra "gótica", a otra "románica"), aun con áreas de jurisprudencia que comienzan a consolidarse de modo interesante (i.e., las referidas a la igualdad de género); y otras varias que parecen ya bien sólidas y resistentes (i.e., las relacionadas con la libertad de expresión, la crítica política, la caricatura, la real malicia, etc.).

La noción de intimidad es un producto cultural, una creación abstracta de la mente humana con fines de preservación, organizativos y evolutivos, y por lo tanto está sujeta a constantes transformaciones adaptables a las necesidades de cada época y lugar. Durante siglos los ámbitos de intimidad que se reconocían de facto o de jure, eran contados y muy sencillos de comprender: el pudor corporal, el secreto confesional, el domicilio y la correspondencia no presentaban mayor dificultad. La irrupción de tecnología y nuevas técnicas de investigación fue volviendo más complejo el asunto. Hoy nos parece indiscutible que las comunicaciones telefónicas deban ser privadas, pero no ocurrió lo mismo con las primeras investigaciones que se valían de su captación. Muestra de esto fue el caso de Roy Olmstead, el ex policía que durante la ley seca se dio cuenta que le resultaba más conveniente ser contrabandista y se pasó de bando creando un cartel con sede en Seattle que fue desbaratado con meses de pacientes escuchas realizadas por agentes federales. A los pesquisas no se les ocurrió que debían pedirle autorización a un juez, porque era algo nuevo, no había ley que lo previera y las comunicaciones de aquella época eran escuchadas por los operadores, y así también lo entendieron los tribunales. La cuestión llegó a la Corte Suprema de Estados Unidos y en 1928 en un ajustado fallo dividido concluyó que Olmstead y los miembros de su banda no tenían un derecho constitucional a la intimidad sobre lo que hablaban por teléfono. Hicieron falta casi 40 años para que el fallo "Katz" fijara la doctrina de la expectativa razonable de privacidad que magistralmente permitió durante

décadas solucionar conflictos con ese derecho. Actualmente, la problemática se agudizó, como sucede con el auge de grandes empresas cuyos algoritmos les permiten guardar, clasificar y procesar datos personales de los usuarios de forma tal que con la actividad digital pueden conocerlos más de lo que se conocen a sí mismos. El avance tecnológico es tan vertiginoso y exponencial, que genera cierto agobio, mareo o desborde que obstaculiza un desarrollo a igual ritmo de las doctrinas que sirvan para comprenderlo en su dimensión y dar soluciones. Tal vez deberíamos empezar a aceptar que el concepto de intimidad cambió profundamente; valga como ejemplo actos que actualmente se comparten a millones de personas y que antes eran profundamente íntimos (peleas de pareja, agonías, cirugías). Y a partir de esa aceptación, reformular el sentido que veníamos dándole al derecho a la intimidad y admitir que es legítimo que la gente use servicios informáticos fabulosos, de alta calidad, pagándolos con privacidad. Después de todo, cuando clickeamos ansiosamente que aceptamos todas las condiciones de uso, que nunca leemos, estamos permitiendo que usen nuestros datos (decimos que si a que accedan a los contactos, fotos, micrófonos, cámara del celular y después nos hacemos los alarmados por el acceso). Y precisamente *the big data* es el gran negocio de las grandes corporaciones. Si las compañías que nos dan *whatsapp, facebook, instagram*, correo electrónico, nubes, orientación satelital, etc., nos tuvieran que cobrar dinero para tener las ganancias que tienen sin usar nuestros datos, posiblemente la mayoría preferiría seguir usándolas con moneda de información. En ningún caso es gratis, y sería absurdo pretender que nos den todo y con la eficiencia que nos lo dan, sin pagar nada de nada, ni un peso, ni un dato. La discusión entonces debe pasar por la forma en la que informan el uso de los datos, los límites y las sanciones para su incumplimiento, pero se acabó la era de la privacidad intensa de los datos personales. En lo que atañe a la instrucción penal, para no estar siempre tan atrasados, deberíamos introducir una fórmula legal amplia en el derecho procesal penal, que prevea la autorización jurisdiccional escrita, fundada en sospechas suficientes, determinada, proporcionada y limitada en el tiempo, para la utilización de medios tecnológicos de investigación de delitos. Con esto se cumple la regla de la taxatividad legal de medidas de injerencia (CADH., 30) y se posibilita el uso de nuevas herramientas. Las regulaciones muy casuísticas o específicas, como la reforma a la ley de enjuiciamiento criminal española de 2015 (arts. 588 y ss.)

tienen el riesgo de quedar obsoletas en pocos años, precisamente por la revolución digital.

2. *Secuestro del aparato telefónico en el marco de un allanamiento domiciliario*

No ofrece mayor dificultad afirmar que si se quieren conseguir pruebas contenidas en un teléfono celular, y este se encuentra adentro de un domicilio, hará falta una orden de allanamiento para su incautación, como con cualquier objeto que pueda servir de prueba. El primer problema que se plantea es si la orden de registro domiciliario para el secuestro de celulares habilita a su inspección; y el segundo radica en el alcance. Como los elementos que serán secuestrados deben ser identificados, inventariados, conservados y ubicárselos dentro de una cadena de custodia, una primera aproximación admite una revisación a tales fines (obtención de número de línea, de IMEI,[421] de SIM, de serie, etc.). Después de todo, esta información no está diciendo demasiado sobre la vida privada del usuario. En esta línea, el Tribunal Su-

[421] "La monitorización es un método tecnológico que permite detectar el número en uso a través del denominado IMEI, que es una clave alfanumérica traducible, posteriormente, a ese número de la terminal, sin intromisión en el contenido del ámbito de la intimidad, es decir, es un acrónimo del inglés que significa Identidad Internacional del Equipo Móvil" (TS Español, resol. 921, 20/10/2009, citando la sentencia del inferior). En casos en que los policías captaron el IMSI sin autorización judicial, mediante la utilización de un escáner en las proximidades del usuario, la Sala Penal del Tribunal Supremo ha considerado que estaban habilitados a hacerlo porque no implica violación al secreto de las comunicaciones, y que el ulterior pedido de informe para la identificación del usuario del IMEI, necesita ser dispuesto judicialmente (Sent. 20/5/2008). Posteriormente, la reforma a la ley de enjuiciamiento de 2015, agregó el art. 588 ter I, estableciendo que siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones, poniendo en conocimiento la utilización de los artificios a que se refiere el apartado anterior.

sea que lo consignó expresamente el magistrado o que en silencio del medio, lo indique el ejecutante.

Podría argumentarse que un programa oculto es en sí mismo ilícito. No es de recibo este argumento porque, en primer lugar, hay aplicaciones informáticas que tienen estas características y no están absolutamente proscriptas (p. ej., los que se dirigen a orientar la publicidad a partir de las búsquedas en internet o las páginas visitadas por el usuario). Y en segundo término, son los propios organismos del Estado los que pueden crear o modificar programas que tengan la finalidad apuntada.

También podría interponerse el reparo de que sería la convalidación del engaño como método de obtención de evidencias (ya sea que se retenga el equipo para la infiltración del programa, se le "obsequie" el aparato, o bien que se lo haga de manera remota enviándole algún archivo ejecutable, etc.). A ello se puede responder que la clandestinidad siempre es una nota característica de la intervención, porque se hacen de manera insidiosa y subrepticia; de lo contrario no tendría ningún resultado y carecería de sentido.

De todas formas, desde el punto de vista constitucional no hay una diferencia cualitativa y sustancial entre la intervención de comunicaciones hecha por el método tradicional y la realizada mediante un programa espía porque los recaudos no varían (orden jurisdiccional, fundada, limitada en el tiempo, determinada, proporcionada) y la materia u objeto de conocimiento generalmente es la misma (las comunicaciones del investigado).

El problema es que los programas espías no solo permiten acceder a las comunicaciones, sino también a todo el contenido del celular (fotos, videos, notas, etc.), entonces si no se filtra o selecciona el alcance de la intromisión, puede ser mucho mayor a la intervención tradicional, sin perjuicio de que los jueces también están habilitados a autorizar el examen de papeles privados, según la antigua denominación.

Como la práctica precedentemente descripta resulta polémica y conflictiva, otros países han incorporado a sus ordenamientos la regulación específica de esta posibilidad. En esta línea, se ubica España, que en 2015 agregó a la ley de enjuiciamiento el art. 588 septies a, estableciendo que el juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico,

sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos: *a)* Cometidos en el seno de organizaciones criminales. *b)* Terrorismo. *c)* Contra menores o personas con capacidad modificada judicialmente. *d)* Contra la Constitución, de traición y relativos a la defensa nacional. *e)* Cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. La resolución debe especificar: *a)* Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida. *b)* El alcance, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información. *c)* Los agentes autorizados para la ejecución. *d)* La autorización, en su caso, para la realización y conservación de copias de los datos informáticos. *e)* Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

En Argentina hay proyectos de reformas que prevén la incorporación de regulaciones sobre la cuestión. Mientras tanto, autorizada doctrina actual opina que desde el punto de vista penal, aun frente a tipos penales como el del art. 153 bis del C.P. (acceso no autorizado a datos), está justificado el ingresar con orden judicial de manera remota a un sistema informático por el cumplimiento del deber.[449]

9. *Geolocalización remota del celular*

Los teléfonos móviles permiten averiguar sus movimientos y ubicación. Ya sea por el área de cobertura de la celda de la antena que capta las comunicaciones, o bien con mucha más precisión por medio del GPS que muchos *smarth phones* tienen.

La discusión sobre la posibilidad policial de rastrear a alguien valiéndose de tecnología que acusa la ubicación, ya ha sido objeto

[449] Pilnik, Franco: *Delitos en el ciberespacio*, Advocatus, Córdoba, 2017, p. 79.

de una extendida elaboración en relación a los seguimientos de personas y vehículos mediante distintos sistemas, particularmente el GPS en los últimos tiempos.

La vigilancia de personas puede recaer sobre sus movimientos, hábitos, relaciones, rutinas, horarios, etc. Pueden involucrar el derecho a la intimidad, pero no cualquier roce sobre este es susceptible de proscribir medidas de investigación sin orden judicial.

Un parámetro de análisis frecuente es el de la "expectativa razonable de privacidad",[450] esto es, cuando sorprende su cuidado, su previsión normal y habitual de un modo que la sociedad reconoce el interés; o si avanza sobre las actividades que legítimamente se quieren sustraer del conocimiento de los demás y se tomaron los recaudos para que esto último no suceda. Pero el cimbronazo que la irrupción de la tecnología viene generando en el derecho a la intimidad, ha llevado a complementar la doctrina de la "legítima expectativa" con la "teoría del mosaico", con la cual se tiene en cuenta el cuadro de conocimiento que cual rompecabezas permite armar el acceso a distintos datos de información personal.

De allí que para determinar cuándo hace falta una autorización judicial, es necesario diferenciar los distintos tipos de seguimientos que pueden presentarse, su impacto en la intimidad personal y qué parte de la vida privada permiten reconstruir. Sobre el particular resulta de aplicación el desarrollo realizado en el capítulo sobre seguimientos a personas y vehículos, particularmente en orden a las vigilancias mediante tecnología.

Llevando la cuestión al terreno del seguimiento valiéndose del aparato de telefonía celular del sospechoso, una primera aproximación permite concluir que el rastreo mediante antenas no afecta una expectativa razonable de privacidad porque solo va a indicar una zona de vías públicas donde estuvo una persona, impidiendo el conocimiento de las visitas a lugares privados que puede haber

[450] Surgido en 1967 del *leading case* "Katz" de la Corte Suprema de EEUU, permite analizar la validez de una intromisión mediante un test subjetivo (si el individuo siente afectada su intimidad) y otro objetivo (si la sociedad reconoce como razonable y digna de protección esa expectativa). La Corte Suprema Argentina y la Cámara de Casación Penal también toman este parámetro al tener en cuenta la "expectativa de intimidad" en el caso concreto como factor de análisis de la validez de un procedimiento (CSJN, *Fallos*, 321:2947; también 12/11/1998 en "Fernández Prieto"; CNCP, Sala I, 4/11/2002, "Bergesio").

realizado y que quiera mantener en un ámbito de intimidad (p. ej., hoteles alojamiento).[451]

Pasando al rastreo mediante GPS o sistemas que con mucha exactitud indican una mapeo constante de la ubicación de una persona por medio del celular que porta, el tema encuentra puntos de contacto con la colocación de un dispositivo en el vehículo o pertenencias del perseguido, pero también diferencias. Un caso de Estados Unidos sirve para ilustrar sobre la discusión.[452] Un detenido acordó convertirse en un informante de la DEA aportando datos en contra del jefe de una organización dedicada al transporte de estupefacientes, indicando que iba a realizarse un traslado entre dos estados, pero ignorando los datos del recorrido. El sindicado usaba celulares descartables registrados bajo falsos nombres. Averiguado el celular del transportista, los policías consiguen un simple oficio del juzgado (no una orden fundada de intromisión) dirigido a la compañía telefónica para que envíe un "ping" (señal) a ese teléfono, y a través del rebote o respuesta automática de esa señal que impactaba en el sistema informático de la empresa prestataria del servicio, los investigadores podían obtener las coordenadas de ubicación del teléfono móvil. De esta manera lograron interceptar el cargamento cuando el transportista había hecho un alto en el camino para descansar, tras lo cual fue detenido y acusado por la confabulación para distribución

[451] En los Estados Unidos una ley federal denominada SCA (Stored Communications Act) le permite al Estado acceder a los registros de conexión de celulares con antenas para establecer ubicaciones, mediante un simple oficio de un juzgado, sin que sea necesaria una orden fundada de injerencia específica. Al respecto, Orin Kerr expone fallos que consideran que el derecho a la intimidad previsto en la cuarta enmienda no abarca esos datos de localización por celdas ("6th Circuit: No fourth amendment rights in cell-site records", The Volokh conspiracy, Abril 2013, The Washington Post, 13/4/2016). Por ejemplo, cita un voto de un fallo ("U.S. Vs. Carpenter", 6th Cir., 2013), en el que se consigna que las cortes federales han distinguido que aunque el contenido de las comunicaciones personales es privado, la información para conectar esas comunicaciones del punto A al B, no lo es. Otro fue el criterio de la Corte al resolver este caso en 2018, considerando la mayoría que el pedido de antenas intervinientes en las comunicaciones del acusado constituyó un registro y por lo tanto requería orden judicial fundada en causa probable (analizaron más de 12.000 ubicaciones durante 4 meses y se lo condenó a 116 años por una serie de asaltos a tiendas Radio Shack y otras en Michigan y Ohio). Para el Presidente de la Corte, el hecho de que la información esté en manos de un tercero no supera al reclamo del usuario a la protección de la Cuarta Enmienda.

[452] "U.S. vs. Skinner", 690 F.3d 772 (6th Cir. 2012).

más de 1.000 kgs. de marihuana. Ante lo moción de supresión de la prueba previa al juicio, el juez de distrito descartó que se hubiese afectado una expectativa legítima de privacidad, sosteniendo que la determinación del dato de ubicación de un celular es simplemente una señal enviada desde una antena de telefonía celular a las computadoras del proveedor del servicio. Después del juicio y la condena, la Corte de Apelaciones confirmó la validez del procedimiento, señalando que no hubo violación a la cuarta enmienda porque no existía una expectativa de privacidad en los datos emitidos por su voluntariamente adquiridos con el plan de celular "pay as you go" (método de prepago sin contrato). Agregó que una herramienta usada para transportar contrabando del que se desprende una señal, ciertamente la policía puede rastrearla. Y citando el caso "Knotts", destacaron que la localización de los datos también podría haberse obtenido por la vigilancia de mera observación visual. Distinguieron el presente caso de la colocación de GPS en un vehículo porque no había ocupación física de la propiedad privada para la obtención de información (como ocurrió en el fallo "Jones"); y solo había durado tres días. En comentario crítico a este fallo se ha señalado que el tribunal describió el proceso seguido para la localización ("pinging") como si fuera pasivo, cuando en realidad no lo era, ya que normalmente los teléfonos equipados con GPS no registran los de localización. Cuando la compañía telefónica fue requerida por el Estado para obtener esos registros, enviaron una señal (o "ping") al teléfono, ordenándole trasmitir su ubicación sin alertar al usuario.[453]

La reforma de 2015 a la ley de enjuiciamiento criminal en España reguló expresamente los seguimientos tecnológicos. Así incorporó el art. 588 quinquies b, estableciendo que cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización. La autorización deberá especificar el medio técnico que va a ser utilizado. Los prestadores de servicios y demás personas físicas y jurídicas están obligadas a prestar colaboración para la ejecución de la medida. Se prevé también que cuando concurran razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y

[453] *Harvard Law Review*, vol. 126, 22/1/2013, p. 807.

localización se frustrará la investigación, la Policía Judicial podrá proceder a su colocación, dando cuenta a la mayor brevedad posible, y en todo caso en el plazo máximo de veinticuatro horas, a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su inmediato cese en el mismo plazo. En este último supuesto, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso.

10. *La incautación de datos en el nuevo Código Procesal Federal*

El nuevo Código Procesal Penal Federal, de diferida implementación, en el art. 151 regula expresamente la incautación de datos, facultando al juez para ordenar, a requerimiento de parte y por auto fundado, el registro total o parcial de un sistema informático, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación. Rigen las mismas limitaciones dispuestas para el secuestro de documentos. El examen del resultado se hace bajo la responsabilidad de la parte que lo solicitó. Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplican las reglas de apertura y examen de correspondencia. El afectado puede recurrir al juez para la devolución de los componentes que no tienen relación con el proceso y la destrucción de las copias de los datos.