JURISPRUDENCIA SOBRE ACCESO A INFORMACIÓN DE CELULARES

"Hoy el gobierno puede escuchar todo lo que digas, sabe dónde estás, con quien hablas, y creéme, sabe con quién te acuestas. Si enciendes un telefóno celular o una computadora estás perdido". Comienzo de la serie "Narcos" que se emite por Netflix.

Ley 25.873. Inconstitucionalidad. Control y almacenamiento de datos de las comunicaciones por 10 años. Celulares. Internet.

Es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos (voto de la mayoría).

Resulta inadmisible que las restricciones autorizadas por la ley estén desprovistas del imprescindible grado de determinación que excluya la posibilidad de que su ejecución concreta por agentes de la Administración quede en manos de la más libre discreción de estos últimos, afirmación que adquiere primordial relevancia si se advierte que desde 1992 es la Dirección de Observaciones Judiciales de la SIDE, que actúa bajo la órbita del poder político, la que debe cumplir con los requerimientos que formule el Poder Judicial en orden a la interceptación de comunicaciones telefónicas u otros medios de transmisión que se efectúen por esos circuitos (voto de la mayoría).

C.S.J.N., 24/2/2009, "HALABI, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986".

Sábanas o listados de comunicaciones. Datos de tráfico. Orden de juez.

Nuestro Máximo Tribunal remarcó que la información del registro de las comunicaciones, es decir la información de las comunicaciones entabladas por el imputado -ya sea duración, geolocalización, personas que tuvieron intercambio, frecuencia de estas, entre otros- gozan de la misma protección que los datos de contenido. Y los unos están indisolublemente unidos a los primeros.

Corresponde destacar que esa conclusión de nuestro Máximo Tribunal no es propia de él sino que así lo ha dicho el Máximo Tribunal Interamericano y la Corte Europea de Derechos Humanos. La primera lo dijo en el caso "Escher" (CIDH, 20/11/2009) y la segunda en el caso "Malone" (TEDH, 2/8/1984). Este último caso cobra trascendencia porque, en lo particular, está emparentado directamente con el caso analizado (en ese caso se condenó al Reino Unido por la utilización de un sistema de conteo de llamadas que registraba en forma automática los datos de los contactos telefónicos entablados sin autorización judicial).

Asimismo, numerosa doctrina nacional e internacional ha avalado esa posición que hace hincapié en que la protección constitucional alcanza a todo el proceso comunicativo y no formula un sesgo sobre el mensaje transmitido (para ver los fallos y la doctrina citada ver BERNARDINI, Pablo A., "La protección constitucional y legal de los registros que contienen los datos externos y de geolocalización de las comunicaciones", Foro de Córdoba, n° 195, septiembre 2018, pág. 47).

Debe existir una equivalencia en la protección de los datos de tráfico y contenido ya que, en caso contrario, un tramo importante del proceso comunicativo que involucra datos sensibles de la persona podría quedar al

descubierto de protección constitucional, siendo que la finalidad del constituyente fue resguardar ese ámbito de autonomía individual de la persona que decide entablar un contacto con otra u otras.

Ante el marco planteado y la omisión evidente del legislador (téngase en cuenta que es un problema que tienen todos los códigos de procedimiento por el contexto de digitalización que estamos viviendo), el riesgo de dejar huérfana de protección un tramo de las comunicaciones, desoír lo que dice la Corte y que ello, a futuro, genere mayor recurribilidad, consideramos que la práctica adecuada debe ser: La información de las comunicaciones existentes en los registros de los proveedores de los servicios correspondientes (datos de tráfico) debe gozar de las mismas condiciones para su autorización que la intervención de comunicaciones (art. 216 del CPP). Es decir, en el mismo sentido como lo regula la legislación adjetiva federal, art. 236 CPPN que ya se hizo mención y en el Código Procesal Penal Federal (ley 27.063) -que sólo se encuentra vigente en algunas jurisdicciones-.

En sintonía con nuestra Corte Suprema, corresponde formular la siguiente aclaración. La anterior pauta –los datos externos de la comunicación que no implican contenido deben ser solicitados por el fiscal de instrucción al juez de control y este debe decidir si da el aval o no- rige de ahora en adelante, es decir un punto de partida en los requerimientos de datos de tráfico.

T.S.J.Cba., Sent. 427, 26/10/2023, "ESTRADA RODRÍGUEZ, Moisés y otra p.ss.aa. tenencia con fines de comercialización -Recurso de Casación-".

Revisación del contenido de celular en allanamiento

El Tribunal Supremo español sostuvo que un allanamiento dispuesto para buscar elementos

relacionados a la investigación incluye la posibilidad de que la autoridad policial comisionada revise el contenido de mensajes telefónicos, porque tal actividad “se encuentra bajo la cobertura de la autorización judicial como si de otro papel o documento se tratara que pudiera relacionarse con el tráfico de las drogas incautadas cuya intervención y "objetos de cualquier tipo relacionados con ellas" constituía el objeto de la diligencia de entrada y registro ordenada por el juez”.

Inspección de celular secuestrado durante allanamiento

El peritaje efectuado sobre los teléfonos incautados en posesión de los imputados, no afecta el derecho de intimidad de éstos ni de otros, si respecto de aquéllos su ámbito privado ya había sido invadido, fundadamente, desde la orden de allanamiento de la morada, acto en el cual se secuestraran los teléfonos celulares peritados, efectuándose sobre ellos un estudio que cabe asimilarlo a aquél que se hace sobre una agenda telefónica.

C.N.C.P., Sala Sala II, 9/3/2011, “OSUNA, Claudio Alberto s/recurso de casación”.

Acceso de policías al contenido del celular de un detenido por irregularidades en la documentación para conducir, de quien surgieron sospechas de pertenencia a una pandilla investigada por delitos

Los datos digitales contenidos en teléfonos móviles conforman una "categoría particular de efectos".

Los teléfonos celulares modernos se han transformado en una parte esencial e importante de la vida cotidiana, al punto que un visitante proverbial de Marte podría concluir que eran una característica importante de la anatomía humana.

Los teléfonos celulares se diferencian tanto en sentido cuantitativo como cualitativo de otros objetos que puedan estar en poder de una persona detenida. El término 'teléfono celular' es en sí mismo engañoso; muchos de estos dispositivos son en rigor minicomputadoras que también tienen la capacidad de ser utilizados como un teléfono. Pudieran fácilmente ser llamados cámaras, reproductores de video, calendarios, grabadoras, bibliotecas, diarios personales, álbumes, televisores, mapas o periódicos.

Uno de los rasgos distintivos de los teléfonos celulares es su inmensa capacidad de almacenamiento. Antes de los celulares, la injerencia en un registro sobre una persona tenía limitaciones físicas y el ámbito de intromisión en la privacidad era en algún punto estrecho, nadie cargaba consigo correos recibidos durante meses, cada imagen que se ha tomado o cada artículo o libro que se ha leído, ni existían razones para hacerlo.

Mientras la regla categórica del fallo "Robinson" logra un equilibrio adecuado en el contexto de los objetos físicos, no parece que este mismo alcance pueda ser aplicable respecto de registros en los que se ingresa en contenidos digitales.

La fiscalía defendió la validez de la inspección en que la información en un teléfono celular puede sin embargo ser vulnerable a dos tipos de destrucción de evidencia: limpieza remota de datos digitales y cifrado de datos. En el caso de barrido remoto, un teléfono, conectado a una red inalámbrica, recibe una señal que borra los datos almacenados. Esto puede suceder cuando un tercero envía una señal a distancia o cuando un teléfono está programado para eliminar los datos al entrar o salir de

ciertas áreas geográficas (el llamado "geofencing"). Por otra parte, el cifrado es una característica de seguridad que algunos modernos teléfonos móviles utilizan, además de la protección de contraseña. Cuando este tipo de teléfonos se bloquea, los datos se convierten en protegidos por encriptación sofisticada que hace que el teléfono sea prácticamente "inaccesible", a menos que la policía cuente con la contraseña.

En respuesta a esa posición, la sentencia remarca que se trataría de acciones ajenas a cualquier intento activo del acusado para ocultar o destruir pruebas después de la detención y la argumentación de la acusación había brindado escasas razones para entender que se trata de un problema frecuente, en todo caso, sólo se dio a conocer un par de ejemplos aislados. Del mismo modo, en el caso del bloqueo por el que la información resulta cifrada, la posibilidad de los oficiales de policía de encontrar la contraseña para acceder a los datos pareciera bastante limitada, considerando, a su vez, que la mayoría de los teléfonos se bloquean con el toque de un botón o como default después de algún período muy corto de inactividad. Por otra parte, en situaciones en las que un arresto podría desencadenar un intento remoto de borrado o un funcionario descubriera un teléfono bloqueado, no está claro que la capacidad de realizar un registro sin orden marcara la diferencia. La necesidad de proceder a la detención, asegurar la escena, entre otras tareas propias de la función, significa que los oficiales encargados de hacer cumplir la ley pueden también no ser capaces de dirigir de inmediato su atención a un teléfono móvil.

La limpieza remota puede ser totalmente impedida con sólo desconectar el teléfono de la red. En primer lugar, los agentes del orden pueden apagar el teléfono o quitar la batería. En segundo lugar, si están preocupados acerca del cifrado u otros problemas potenciales, pueden dejar el teléfono encendido y colocarlo en un recinto que aísle el teléfono de las ondas de radio.

Si la policía está verdaderamente enfrentando una situación de 'ahora o nunca' —por ejemplo, ante circunstancias que sugieren que el teléfono de un acusado será objeto de un control remoto inminente que destruirá la información—, los oficiales de policía están habilitados a confiar en esas circunstancias extremas para registrar el teléfono inmediatamente. Si los oficiales secuestran un teléfono en un estado desbloqueado, están habilitados a desactivar la función de bloqueo automático con el fin de evitar su bloqueo y el cifrado de datos.

Si bien un detenido ve disminuida la protección de su privacidad, esto no significa que pierda la protección de la IV enmienda. No todo registro es permitido por el hecho de que la persona se encuentre bajo custodia.

La capacidad de almacenamiento de los teléfonos celulares tiene varias consecuencias relacionadas con la vida privada. En primer lugar, un teléfono celular acumula en un solo lugar muchos tipos distintos de información —una dirección, una nota, una receta, un estado de cuenta bancario, un vídeo— que revelan mucho más en combinación que cualquier registro aislado. En segundo lugar, la capacidad de un teléfono celular le permite que incluso un solo tipo de información transmita mucho más de lo que antes era posible. La suma de la vida privada de un individuo puede ser reconstruida a través de un millar de fotografías etiquetadas con fechas, lugares y descripciones; lo mismo no puede decirse de una o dos fotografías de sus seres queridos guardados en una cartera. En tercer lugar, los datos de un teléfono pueden remontarse a la compra de ese teléfono, o incluso antes. Una persona puede llevar en el bolsillo un papelito que le recordaba llamar al señor Jones; él no llevaría un registro de todas sus comunicaciones con el Sr. Jones durante los últimos meses, como rutinariamente se mantiene en un teléfono".

El monitoreo GPS genera un registro preciso y completo de movimientos públicos de una persona que refleja una gran cantidad de detalles sobre

sus vínculos familiares, políticos, profesionales, religiosos y sexuales" (cita del caso “Jones”).

Las exigencias que impone este fallo es el costo para preservar la privacidad que se protege constitucionalmente contra registros irrazonables. Los oficiales de policía cuentan hoy con medios tecnológicos (e-mail, ipad's, incluso sus propios smartphones, etc.) con los que, frente a presupuestos que ameriten el registro del contenido de un celular, pueden efectuar adecuadamente su requerimiento, obteniendo una respuesta en prácticamente quince minutos y, para el caso de enfrentar situaciones de extrema urgencia, tienen siempre disponible la excepción a la obligación de requerir orden judicial de registro.

Nuestra respuesta a la pregunta de lo que la policía debe hacer antes de registrar un teléfono celular incautado en un incidente de arresto es simple: obtener una orden judicial.

CSEEUU., 25/6/2014, "Riley vs. California"[1].

Captación remota de IMEI

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.

[1] Comentario y traducción de Carral, Daniel, “¿Smartphones con garantía extendida?”, Revista de Derecho Penal y Procesal Penal Abeledo Perrot N° 7, 2015, ps. 1404 y ss.

No cabe hablar de las referidas vulneraciones constitucionales, toda vez que la actividad investigadora, en este caso, no llega a afectar al núcleo protegido por los derechos fundamentales.

Lo trascendente del contenido digno de protección por parte del derecho al secreto de las comunicaciones ha de ser aquello que, en realidad, pueda llevar a calificar la injerencia como verdaderamente gravosa en el ámbito personal del investigado, es decir, los contenidos ideológicos de esa comunicación, los mensajes y el intercambio de ideas, opiniones, pensamientos, sentimientos, etc., que constituyen la esencia de la misma.

Los números identificativos con los que operan los terminales no pueden constituir, por sí mismos, materia amparada por el secreto de las comunicaciones, pues afirmar lo contrario supondría confundir los medios que posibilitan la comunicación con la comunicación misma. Sostener semejante criterio no supone contradicción alguna, con la doctrina del TEDH contenida en el caso “Malone", ni con la del Tribunal Constitucional ni, mucho menos aún, con la de esta misma Sala, pues esa doctrina se refiere a la extensión del ámbito protegido de la "comunicación" no tanto a los números telefónicos sino al hecho de que, a través de la averiguación de esos números, se conozcan extremos como el momento, la duración y, lo que es aún más importante, la identidad de las personas que establecen el contacto. Y eso sí que puede sostenerse que forma parte, auténticamente, de la "comunicación".

TSEspaña, Res. 921, 20/10/2009.

Geolocalización del celular. Rastreo del transportista que trasladaba cargamento de estupefacientes mediante oficio 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.

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.

No hubo violación a la cuarta enmienda porque no existió 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).

Un instrumento usado para transportar contrabando del que se desprende una señal, ciertamente puede ser rastreado por la policía.

La localización de los datos también podría haberse obtenido por la vigilancia de mera observación visual.

El caso se distingue de la colocación de GPS en un vehículo porque no hubo ocupación física de la propiedad privada para la obtención de información y sólo duró tres días.

C.Apel. 6th Cir., "U.S. vs. Skinner", 690 F.3d 772 (2012).

Asaltos en series a tiendas electrónicas en distintos lugares. Localizaciones de celulares de sospechosos por las antenas. Obtención de 12,898 puntos de ubicación de los movimientos del imputado durante 127 días (un promedio de 101 por día).

La Corte de Apelaciones del 6° Circuito había sostenido que el imputado carecía de una expectativa razonable de privacidad en la localización de la

información colectada por el FBI porque él había compartido esa información con sus proveedores inalámbricos.

La adquisición de los registros de sitios de celdas fue una injerencia en los términos de la Cuarta Enmienda. Cuando un individuo buscar preservar algo como privado y su expectativa de privacidad es una de aquellas que la sociedad está preparada para reconocer como razonable, la intromisión oficial en esa esfera generalmente se califica como un registro y requiere una orden judicial sustentada en causa probable.

Los datos digitales en cuestión –ubicación personal mantenida por una tercera parte no se ajusta exactamente a los precedentes existentes, pero coincide en la intersección de dos tipos de casos. Uno concierne a la expectativa de privacidad sobre la ubicación física y los movimientos (United States v. Jones, 565 U. S. 400 en el que concluyeron que la privacidad debe ser protegida del rastreo intensivo por GPS colocado en vehículo). La otra se relaciona con la expectativa de privacidad en la información voluntariamente entregada a una tercera parte (United States v. Miller, 425 U. S. 435 sentando que no hay expectativa de privacidad en ciertos datos financieros mantenidos por un banco).

Los individuos tienen una expectativa razonable de privacidad en el conjunto de sus movimientos físicos. Permitir que el Estado acceda a los registros de los sitios de celulares –para muchos americanos "las intimidades de su vida"- contraviene esa expectativa.

El Estado respondió que los datos CSLI son menos precisos que la información del GPS pero consideró que los datos eran lo suficientemente precisos. De todos modos, la regla que la Corte adopta debe tener en cuenta a sistemas más sofisticados que están actualmente en uso y que la precisión del CSLI está rápidamente acercándose al nivel del GPS.
La fiscalía respondió que la doctrina de la tercera parte debía regir este caso porque los datos de ubicación de celdas son registros comerciales

creados y mantenidos por las empresas. Pero hay un mundo de diferencia con la crónica exhaustiva de la información de locación colectada. La doctrina de la tercera parte se basa en la noción que un individuo tiene reducida la expectativa de privacidad en la información que a sabiendas compartió con otro.

CSEEUU, 22/6/2018, “Carpenter vs. U.S.”.