Comisión 2. Procesal Penal. Jurisdicción y nuevas tecnologías.

Tema. La protección constitucional y legal de los registros que contienen los datos externos y de geolocalización de las comunicaciones.

Apellido y nombre del autor. Bernardini, Pablo Andrés

Dirección postal. Lote 20 Manzana 214, La Estanzuela I, La Calera, Depto Colón, Pcia. De Córdoba, C.P. 5151.

Teléfono. 0351-156333380

Dirección de correo electrónico del autor. pablobernardini70@hotmail.com

Breve síntesis de la propuesta. El trabajo propone un análisis dentro del marco normativo argentino de la protección constitucional y legal que tienen los registros que poseen las empresas proveedoras de servicios sobre los datos externos y de geolocalización de las comunicaciones. A los fines de una mayor riqueza del tratamiento se hace mención al tema en España y Estados Unidos. Posteriormente se hacen algunas consideraciones sobre cómo debería ser el dictado de la medida en la provincia de Córdoba que cuenta con una normativa diferente a la del Código Procesal Penal de la Nación.

I. Introducción

El presente trabajo tiene por finalidad analizar de acuerdo al marco normativo argentino cuál es la protección que tienen los datos de tráfico o metadatos y, datos de geolocalización (información que queda asentada en los registros de las compañías que proveen los respectivos servicios de comunicación) y si para su otorgamiento basta con la solicitud de un fiscal o si es necesaria una resolución de un Juez. A los fines de un tratamiento más amplio del tema, también se hará un breve análisis sobre la problemática en cuestión en España (con referencia al Tribunal Europeo de Derechos Humanos) y Estados Unidos.

II. La protección de la intimidad. La inviolabilidad de las comunicaciones. Normativa constitucional y supra constitucional. Leyes infraconstitucionales. Constitución de Córdoba. La cuestión en España y Estados Unidos

Nuestra C.N. protege el derecho a la intimidad en forma expresa en el art. 19 1º párrafo. También se otorga protección al derecho a la intimidad en el artículo 18 al asegurar la inviolabilidad del domicilio, de los papeles privados y de la correspondencia epistolar.

Los tratados internacionales, que forman parte de nuestra Constitución Nacional de acuerdo al art. 75 inc. 22, contienen similares normas. El art. 5 de la Declaración Americana de los Derecho y Deberes del Hombre y el art. 12 Declaración Universal de Derechos Humanos abordan el tema. Asimismo, los artículos 17.1 y 17.2 del Pacto Internacional de Derechos Civiles y Políticos. A su vez, el art. 11 de la Convención Americana sobre Derecho Humanos contienen reglas al respecto.

A los fines de precisar los alcances de tal normativa, la Corte Suprema al analizar un caso sobre intervenciones telefónicas sostuvo que “si bien allí no se hizo mención a las comunicaciones telefónicas ni a la protección de su secreto, una interpretación dinámica de su texto más lo previsto en el art. 33 y en los

artículos 11, inciso 2º, de la Convención Americana sobre Derechos Humanos y 17, inciso 1º del Pacto Internacional de Derechos Civiles y Políticos permiten hacer aquellas consideraciones a casos como el presente"[1]. En esa línea, la CIDH en el caso "Tristán Danoso vs Panamá"[2] dijo que tal forma de comunicación se encuentra incluida dentro del ámbito de protección de la vida privada.

En cuanto al contenido de dicha protección, la Corte Suprema –caso Halabi[3]- y la CIDH (caso Escher vs Brasil) se han encargado de destacar que la protección legal que da la inviolabilidad de las comunicaciones abarca a todo el proceso comunicativo. Esto quiere decir que el resguardo legal del derecho enunciado comprende desde que se envía el mensaje hasta que llega al receptor, incluyendo los datos que forman parte de ese proceso independientemente de si se logra conocer el contenido de lo comunicado[4].

En el sistema normativo argentino encontramos mención a la inviolabilidad de las comunicaciones en la ley de Inteligencia 25.520 –art. 5- y en la nueva ley de Telecomunicaciones 27.078 –art. 5-.Como advierte García, desde la entrada en vigencia de dicha norma, se declara la inviolabilidad no sólo de las telecomunicaciones, sino de los archivos de registro, y se requiere orden o dispensa judicial para acceder a ellos o darlos a conocer[5]. Pablo Palazzi al respecto señala que "En la Argentina ambas clases de datos -los de

---

[1] CSJN "Quaranta" (*Fallos*: 333:1674).

[2] CIDH, Sentencia del 27/01/2009.

[3] CSJN "Halabi" (Fallos 332:111).

[4]CIDH, Sentencia del 20/11/2009, Escher vs Brasil, parágrafo 114, al mencionar el marco normativo en que se enmarca el conflicto tratado.

[5] García, Luis M., *"La vigilancia de las telecomunicaciones y otras comunicaciones interpersonales según la jurisprudencia elaborada en torno al Código Procesal Penal de la Nación"*, en *"Garantías constitucionales en la investigación penal"*, Florencia G. Plazas, Luciano A. Hazán (Comps.), Del Puerto – Bs. As. – 2006, p. 313.

tráfico y los del contenido de la comunicación- están amparados por el art. 18 CN. y su intervención requiere la correspondiente orden judicial"[6].

En lo que refiere a la ley que regula las telecomunicaciones en Argentina –la ley 27.063 denominado "Argentina digital" contempla en su artículo 5 la inviolabilidad de las comunicaciones. "Su interceptación, así como su posterior registro y análisis, sólo procederá a requerimiento de juez competente".

De una lectura de la legislación se advierte, que no se hace mención a la protección de los registros que contienen los datos externos de una comunicación. De manera que, la protección que se consagra en la ley de inteligencia 25.520 es más amplia que esa normativa y respeta los parámetros establecidos por la Corte Interamericana en el caso Escher. Ello motivó la crítica de diversas ONG, que han hecho saber su descontento con la nueva legislación:"[7].

En lo que refiere a la Constitución de Córdoba, el constituyente ha previsto una fórmula legislativa que establece que el secreto de cualquier forma de comunicación personal por el medio que sea es inviolable. Posteriormente señala una "ley determinará los casos en que se puede proceder al examen e interceptación mediante orden judicial motivada".

En España, la jurisprudencia del Tribunal Constitucional y Tribunal Supremo se han encargado de proteger el derecho al secreto de las comunicaciones que cubre no sólo el contenido de la comunicación sino que abarca a todo el proceso comunicativo. Tiene como base que en la constitución española, el art. 18.3 contempla el derecho al secreto de comunicaciones y que la jurisprudencia del Tribunal Europeo de Derechos Humanos[8] ha remarcado la

[6]PALAZZI, Pablo A., "La regulación de los datos de tráfico en la Argentina: comentario a la ley 25.873", SJA 5/5/2004- JA 2004-II-1346.

[7]http://www.enredando.org.ar/2014/11/25/la-adc-y-la-fundacion-via-libre-manifiestan-su-preocupacion-por-el-dictamen-de-argentina-digital/La protección de los registros de metadatos en la argentina

[8]TEDH , Malone vs. Reino Unido, 02/08/1984.

necesidad de proteger las comunicaciones de esa manera. Al realizar la justificación del alcance de esta garantía señala el Tribunal Supremo agrega “en una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo”.

La Constitución de los Estados Unidos cuenta con la Cuarta Enmienda que establece el derecho de los habitantes a la seguridad en sus personas, domicilios, papeles contra registros y secuestros arbitrarios, es inviolable. En materia de los registros que quedan de las comunicaciones, existe una ley “Stored Communication Act”, que establece los requisitos que tienen que reunir los operadores del sistema para solicitar las mismas.

III- Registro de las comunicaciones. Datos personales. Importancia.

En primer lugar, a los fines de observar el peso que tiene estos datos, un estudio realizado por dos investigadores de la Universidad de Stanford en 2014[9] mostró que el análisis de los llamados Metadatos de un teléfono celular –sin incluir el contenido- que incluyen el iniciador, el destinatario, el horario y la duración de las comunicaciones revelan detalles personales íntimos sobre los propietarios del teléfono. También merece destacarse que en un proceso de consulta, liderado por las organizaciones Privacy International Access y Electronic Frountier Foundation y co firmados por más de trescientos organizaciones de todo el mundo, se elaboraron los “Principios Internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones”. En la explicación de los motivos del proyecto se ha

[9] Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, WEB POL’Y (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the -sensitivity-of-telephone-metadata, citado por SCHLABAG, Gabriel R. “Privacy in the cloud: the mosaic theory and the Stored Communications Act”, Stanford Law Review, Volumen Nº 677, págs. 677/721 extraído del sitio web http://www.stanfordlawreview.org/sites/default/files/67_Stan_L_Rev_677_Schlabach.pdf pág. 688.

destacado, con citas de estudios tecnológicos que “Los metadatos de las comunicaciones pueden crear un perfil de la vida de un individuo, incluyendo condiciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tan o, incluso, más detalladamente de lo que sería posible desde el contenido de las comunicaciones”[10].

IV.Tratamiento del tema en España, jurisprudencia europea y Estados Unidos. Protección constitucional y legal. Organismos autorizados para solicitar los registros de las comunicaciones

En la sentencia del año 1984 –caso Malone vs Reino Unido[11]- el TEDH dedicó un apartado íntegro al estudio de la naturaleza de los datos obtenidos mediante el llamado procedimiento de “recuento” (un contador combinado con un aparato impresor) que registra los números marcados en un determinado aparato telefónico, la hora y duración de la llamada. Al establecer estos registros, el organismo encargado de ello –Post Office-, utilizó únicamente las señales que se le habían dirigido para asegurar el servicio de teléfono y no vigiló ni interceptó de ninguna manera las conversaciones. El Tribunal señaló que la utilización de los datos así obtenidos ponerlos en conocimiento de la policía sin el consentimiento del abonado se opone al artículo 8 del CEDH.

El Tribunal consideró en el caso “Copland”[12] que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por internet de la demandante, sin su conocimiento, constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia[13].

---

[10] https://es.necessaryandproportionate.org/text

[11] TEDH “Malone vs. Reino Unido”, 02/08/1984.

[12] TEDH “Copland vs. Reino Unido”, 03/04/2007.

[13] Epígrafe 43 del fallo mencionado del TEDH.

La jurisprudencia del Tribunal Supremo español no ha sido tan exigente como las resoluciones anteriormente señaladas. Dicho Tribunal admitió en un supuesto que "la resolución judicial para solicitar la información a la compañía telefónica puede, excepcionalmente, revestir forma de providencia en atención a la menor intensidad de la afectación al derecho fundamental". Y en otra posterior, quitan el tenor de protección que había afirmado el TEDH (Resoluciones 2384/2001 y 1086/2003). Entienden que la diligencia sobre el listado de llamadas no supone ninguna intromisión en el derecho a la intimidad, ya que han sido obtenidas en legal forma y sólo sirven para acreditar los usuarios de los teléfonos intercomunicados, sin entran en el contenido de las conversaciones". Esta jurisprudencia ha motivado la crítica de varios autores[14].

En los Estados Unidos se ha abordado la temática desde dos puntos de vista. En primer término se ha hecho hincapié en que la información que contienen los proveedores de los servicios de comunicación ha sido cedida voluntariamente por los usuarios a las empresas, por lo tanto no gozan de la protección de la cuarta enmienda.

En segundo lugar, en recientes pronunciamientos sobre la temática se ha utilizado la teoría del mosaico –consistente en un análisis amplio para determinar si el volumen de información almacenada y analizada permite aportar datos sobre la intimidad de la persona- para, de esta forma, dirimir si existen violaciones a la Cuarta Enmienda. Ello toma como referencia el caso US Vs Jones de la Corte Suprema, que abordó la cuestión si la instalación de un

[14]RIVES SEVA, Antonio Pablo, obra citada, pág. 317 y SÁNCHEZ SIASCART, obra citada. LÓPEZ BARJA DE QUIROGA, Jacobo *"Actuaciones policiales y el control judicial en el ámbito informático y de las telecomunicaciones. Regulación en el ordenamiento español"*, Revista de Derecho Procesal Penal, Editorial Rubinzal Culzoni, págs. 41/76 realiza un análisis exhaustivo sobre los fallos del Tribunal Supremo relativos a la actuación policial en el ámbito de las telecomunicaciones y su validación sin orden judicial, concluyendo que siempre debe exigirse la autorización judicial para que la fuerza policial obtenga datos relativos a cualquier tipo de comunicación.

dispositivo GPS durante más de 30 días necesitaba autorización judicial ya que contaba con protección constitucional[15].

En relación a la doctrina de la información cedida a "terceras partes" desde finales de los 70, la Suprema Corte ha sostenido que la Cuarta Enmienda no brinda, protección a la información compartida por los usuarios de servicios a las compañías proveedoras de servicios –(caso US vs Miller[16], y en Smith vs. Maryland[17]). El máximo Tribunal de Estados Unidos utilizando el precedente "Katz", consideró dudoso que los usuarios de teléfonos tuviesen alguna "expectativa real de la intimidad en los números que marcan", ya que ellos saben que deben compartir esa información con la compañía telefónica para iniciar llamadas.

Recientemente, la cuestión sobre los registros de un teléfono móvil –metadatos y datos de geolocalización- fue abordado por la Corte de Apelaciones del Quinto Circuito[18]. Dicho Tribunal sostuvo que el gobierno podía acceder a los registros de los datos históricos del celular sin una "warrant" y a través de una "court order" de acuerdo a la legislación "Stored Communication Act". La diferencia entre una y otra consiste en que la primera requiere prueba para su otorgamiento a diferencia de la segunda que sólo requiere que se expliciten los motivos para su concesión.

V. La situación en Argentina

[15]Para ver un análisis sobre el fallo US Vs Jones ver BERNARDINI, Pablo *"El seguimiento y vigilancia de personas a través del dispositivo GPS (sistema de geoposicionamiento satelital): traducción y comentario del fallo Jones vs. U.S., de la Corte Suprema de los Estados Unidos"*, Cuestiones de intervenciones policiales II, Editorial Mediterránea, 2014, págs.. 313/337.

[16] United States v. Miller, 425 U.S. 435, 440-43 (1976).

[17] Smith v. Maryland, 442 U.S. 735, 745- 746 (1979).

[18] 724 F.3d 600 (5th Cir. 2013).

Como ya se destacó en la primera parte, la ley 27.078 establece la inviolabilidad de las comunicaciones, pero no precisa el alcance de dicho término.La ley de inteligencia sí precisa que el derecho a la inviolabilidad de las comunicaciones alcanza a todo el proceso comunicativo. Con respecto a los registros que quedan de las comunicaciones, en la República Argentina la ley 25.326 de protección de datos personales no define la cuestión, aunque el trámite parlamentario dejo expresamente de lado la posibilidad de considerar el número de teléfono como un dato de acceso público[19]. En el ámbito administrativo, Iglesias nos señala que la autoridad de aplicación ha mantenido silencio respecto al carácter personal de los datos de tráfico[20].

Respecto al almacenamiento y acceso, el congreso argentino sancionó la ley 25.873, que modificó la ley 19.728 incorporando dos artículos identificado como *45 bis y ter* regulando la captación y derivación de comunicaciones para su observación remota por parte de organismos de seguridad, estableciendo la obligación de los proveedores de internet de mantener los datos de tráfico por el término de diez años. El decreto reglamentario, identificado con el número 1563/2004, establecía un mecanismo de acceso a los mismos en el que se omite mención alguna a la necesidad de orden judicial como requisito previo.

Esto llevó a la impugnación de la constitucionalidad de dichas normas in re *"Halabi c/PEN s/Amparo*", fallo que acogió por primera vez una acción colectiva en la jurisprudencia argentina. Respecto al tema de la constitucionalidad de la regulación del secreto de las comunicaciones, el supremo tribunal resolvió en contra de la validez de la norma argumentando

---

[19]GILS CARBÓ, Alejandra M, "*Régimen Legal de las Bases de Datos y Hábeas Data*", Editorial LA LEY, 2001, citada por IGLESIAS, Gonzalo "Inviolabilidad de la correspondencia y comunicaciones electrónicas en el derecho argentino" artículo publicado en la Edición Nº 10 - Diciembre 2011 - de **la** Revista Digital ElDerechoInformatico.com

[20] IGLESIAS, Gonzalo "Inviolabilidad…"cit.

que la recolección de datos de conexión invade los derechos consagrados en el art. 18 de la constitución.

V.- ¿Está facultado el fiscal para solicitar la medida analizada?

En la jurisprudencia europea y estadounidense citada anteriormente vimos los organismos que se encuentran legitimados para solicitar los registros de las comunicaciones. En el caso de España el juez, en el de Estados Unidos –con la crítica que ello trae- las fuerzas policiales deben solicitar al magistrado una "court order" que no requiere "probable cause".

Como se reseñó anteriormente al hablar sobre la protección legal con que cuentan la inviolabilidad de las comunicaciones en nuestro sistema, se hizo mención a que el art. 5 de la ley de inteligencia establece como requisito para la procedencia de la medida "orden o dispensa judicial". Para Palazzi se allí se desprende que debe ser por orden del juez[21]. La redacción parece permitir que sea dictada por un fiscal y no excluyentemente por el juez.

En lo que refieren a las leyes de procedimiento, en el orden federal contamos con una norma que establece expresamente que los registros de las comunicaciones los debe solicitar el juez (Artículo 236, 2do. párrafo del CPPN). la CSJN en el ya mencionado fallo Halabi (confr. art. 236, segunda parte, del Código Procesal Penal de la Nación, según el texto establecido por la ley 25.760)", norma que concuerda con el artículo 18 de la ley 19.798.

A diferencia del procedimiento federal, en el caso de la Provincia de Córdoba, no contamos con esa norma. El ordenamiento procesal cordobés no establece que sea un juez el que deba pedir esos registros. La constitución de nuestra provincia establece que "la ley determina los casos en que se puede proceder al examen o interceptación mediante orden judicial motivada" y el art. 216 del Código Procesal Penal establece que para la intervención de las comunicaciones "el Tribunal" deberá ordenar por decreto fundado.

[21] PALAZZI, Pablo A., "La regulación…" cit.

Al respecto, Sebastián Romero quien efectúa un análisis comparativo de las legislación federal y la de la provincia de Córdoba con respecto al pedido de sábanas telefónicas, haciendo alusión a los procedimientos provinciales, concluye que "se desprende, con toda claridad, que el requerimiento de registros de comunicaciones telefónicas forma parte de extenso catálogo de medidas, no enumeradas taxativamente, que el fiscal puede disponer por sí, en tanto no ha sido reservada expresamente por la ley al juez. Tampoco dicha exigencia surge, y he aquí el meollo de la cuestión, de las normas constitucionales que han sido ya examinadas. Es por ello precisamente que el legislador procesal no se encuentra condicionado en este punto, como sí ocurre con la intervención de comunicaciones"[22]. Como se puede ver, el ordenamiento procesal cordobés no contiene una normativa que obligue a que los datos externos de las comunicaciones sólo puedan ser autorizados por el Juez.

Sin embargo, al no contar con una regulación específica la medida señalada, considero necesario hacer algunas aclaraciones, sobre el dictado de la misma por parte del Fiscal. Al ordenar la medida el representante del Ministerio Público tiene que realizarla a través de un "decreto fundado" y contando con elementos suficientes para sospechar que de esos datos externos de la comunicación pueden aparecer información de relevancia para la investigación. Ello porque, como se explicitó anteriormente la garantía de la inviolabilidad de las comunicaciones –que incluye los datos externos y de geolocalización- opera como un límite a las injerencias que puede realizar el estado sobre la privacidad del ciudadano. De lo contrario, otorgar la medida analizada a través de un simple decreto y sin aval probatorio desconocería el alcance de la garantía constitucional de inviolabilidad de las comunicaciones con el alcance que se indicó anteriormente.

---

[22] ROMERO, Gerardo Sebastián, *"Los registros de comunicaciones telefónicas ("sábanas") en la investigación penal: otro capítulo sobre la permanente tensión entre tecnología y privacidad"*, Revista de Derecho Procesal Penal N 2, 2011, Editorial Rubinzal Culzoni.