ISSN 3008-9484 | DOI 10.5281/zenodo.17967042 **Diálogos y Voces Judiciales |** Vol. 2, Núm. 3 (diciembre de 2025): 61-71

LA INVESTIGACIÓN CRIMINAL EN BASE AL ANÁLISIS DE LAS COMUNICACIONES: UN MÉTODO

Criminal Investigation Based on Communications Analysis: A Method

Maximiliano Rubén Gomez[*] y Francisco Brocca[**]

Universidad Nacional del Oeste

mrgomez@mpba.gov.ar / fbrocca@uno.edu.ar

RECIBIDO 06/11/2025 - ACEPTADO 17/11/2025

Resumen

La evolución constante de las modalidades delictivas exige adaptar las herramientas tecnológicas aplicadas a la investigación penal. En este contexto, el análisis de comunicaciones puede resultar determinante para establecer la intervención y autoría en hechos ilícitos, aunque su complejidad técnica dificulta su comprensión y valoración probatoria. Por ello, se vuelve esencial contar con un método de investigación claro y estructurado que asista a analistas y operadores del sistema penal.

Palabras clave:

Método, análisis de las comunicaciones telefónicas, investigación, garantías constitucionales.

Abstract

The constant evolution of criminal modalities demands the adaptation of technological tools used in criminal investigations. Communication analysis can be decisive in establishing involvement and authorship in unlawful acts, although its technical complexity hinders both understanding and evidentiary assessment. Therefore, a clear and structured investigative method becomes essential to support analysts and practitioners within the criminal justice system.

Keywords:

method, communication analysis, investigation, constitutional rights.

1. Introducción

En los tiempos actuales el acceso a las nuevas tecnologías de comunicación pone de manifiesto el avance de un cambio de paradigma, sobre todo en el aspecto de la investigación

[*] Ayudante Fiscal U.F.I Nro. 7 de MGR. Abogado con distinción de diploma de honor (UBA). Especialista en Derecho penal y en Litigio Penal (UBA). Diplomado en Sistema Penal y Nuevas modalidades delictivas, en Derecho Constitucional y Magistratura y en Derechos Humanos control de Convencionalidad y Constitucionalidad Universidad Nacional del Oeste. (UNO). Ayudante docente en Teoría del Delito (UBA). Profesor de IUNMA en Derecho Penal Parte Especial. Profesor de Estado y Sociedad, Política Criminal y del Seminario de gestión Policial-Judicial del (IUV). Profesor de las materias Derecho Penal I, Derecho Procesal Penal, Derecho Penal Parte Especial y Taller de investigación Criminal I y II de la Tecnicatura Universitaria en Investigación Criminal (UNO). Director de la Diplomatura Universitaria en Investigación Criminal (UNDELTA). Investigador de la Universidad Nacional del Oeste.

[**] Secretario de la U.F.I. Nro. 1 de Trenque Lauquen. Abogado de la Universidad de Buenos Aires (UBA). Diplomado en Sistema Penal y Nuevas modalidades delictivas; en Derecho Constitucional y Magistratura; y en Derechos Humanos control de convencionalidad y constitucionalidad; todas de la Universidad Nacional del Oeste. (UNO). Ayudante docente en Derecho Internacional Público (UBA, 2017-2023). Jefe de Trabajos Prácticos en Derecho Internacional Público (Universidad Dr. Plácido Marín, 2021-2023). Profesor de las materias Derecho Procesal Penal, Investigación y Derechos Humanos y Taller de Investigación Criminal 1 de la Tecnicatura Universitaria en Investigación Criminal (UNO).

criminal. Algo tan simple como un teléfono celular inteligente nos permite comunicarnos con personas a miles de kilómetros de distancia, a través de mensajes multimedia, navegación en internet, y el registro de sus ubicaciones, entre tantas otras cosas.

En otras palabras, las nuevas tecnologías han cambiado la forma de relacionarse entre las personas. Sin embargo, no todo es color de rosa. Estas tecnologías han provocado una expansión en el ámbito jurídico penal, no sólo en las investigaciones, sino que han proliferado nuevas modalidades delictivas digitales (defraudaciones informáticas, *grooming*, robo de datos, etc.). En tal sentido, estas nuevas herramientas son utilizadas para el funcionamiento de bandas criminales, las cuales han ido perfeccionando su uso para la comisión o encubrimiento de delitos. En contrapartida, el análisis de los teléfonos celulares de los imputados se vuelve un elemento clave en la investigación, como así el estudio de toda la evidencia digital que él contenga.

Intentaremos, a lo largo del presente artículo, establecer cómo una de las aristas de la evidencia digital, las telecomunicaciones, se impone como de vital interés para las investigaciones criminales. Además, propondremos un método de investigación para su análisis que podría resultar superador para la eficiencia investigativa.

2. El análisis de las comunicaciones

Si bien el objetivo central del presente es el análisis de las telecomunicaciones, no podemos pasar por alto el concepto de evidencia digital y sus diversas acepciones. En tal sentido, como primera aproximación podemos definir la evidencia digital como cualquier información sujeta a una intervención humana, electrónica y/o informática que ha sido extraída de un medio tecnológico informático; por ejemplo: computadoras, celulares, aparatos digitales, medios ópticos. Técnicamente es un tipo de evidencia física que puede ser recolectada y analizada con herramientas y técnicas especiales (Ministerio de Seguridad de la Nación, 2023, p. 5).

En consecuencia, podemos decir que la evidencia digital es todo dato o conjunto de datos informáticos introducidos en un proceso con fines probatorios, que pueda provenir de archivos, registros, mensajes electrónicos, registros de actividad en línea, metadatos, imágenes, y cualquier otro dato almacenado en dispositivos electrónicos o sistemas informáticos ("Protocolo de gestión de almacenamiento de la evidencia digital", MPF de CABA, 2013, p. 2). Al ser el análisis de la evidencia digital una pieza importante para el esclarecimiento de los delitos, así como para determinar el grado de participación de las personas imputadas, resulta primordial que la obtención de dichos indicios se haga respetando todas las garantías que rigen el proceso penal.

La discusión posee relevancia directa en el ámbito de injerencia sobre diferentes derechos consagrados tanto nacional como internacionalmente. Tal es así que no sólo pueden verse afectadas garantías constitucionales que rigen en el proceso penal a nivel nacional (arts. 18, 19 y 33 de la Constitución Nacional), sino también toda la normativa internacional existente al respecto, como ser el art. 11 incisos 2 y 3 de la Convención Americana sobre Derechos Humanos, art. 17 del Pacto Internacional de los Derechos Civiles y Políticos, art. 12 de la Declaración Universal de Derechos Humanos y 10 de la Declaración Americana sobre Derechos Humanos.

Dichos artículos, conforman el plexo normativo que funciona como escudo contra la interceptación de las comunicaciones y la protección del ámbito de privacidad de todas las personas, sin distinción alguna. Nuestra Constitución establece particularmente al respecto que sólo una orden emitida por un juez o una ley que así lo dictamine, podrá hacer cesar este escudo de inviolabilidad de las comunicaciones, que es lo que sucede, por ejemplo, con la Ley Nacional de Telecomunicaciones o el Código Procesal Penal de la Provincia de Jujuy.

En ese camino, y en relación al punto central del análisis de las comunicaciones, el Código Procesal Penal de la Provincia de Jujuy, en su artículo 231, establece que las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal y ser pasible de la imposición de multas a favor del Ministerio Público de la Acusación conforme la reglamentación que se dicte al efecto.

Este artículo evidenciaría que es el Ministerio Público Fiscal quien puede –y debe– solicitar la información de las comunicaciones telefónicas de los investigados, estableciendo que las compañías deberán facilitarle la información. A diferencia de ello, el articulado del Código Procesal Penal de la Provincia de Buenos Aires no especifica quién debe realizar el pedido de información de las telecomunicaciones. Por ello es que, resulta propicio destacar lo expuesto por los jueces la Sala I del Tribunal de Casación Penal de la Provincia de Buenos Aires en la sentencia número 68962 "L.M.A s/Recurso de Casación".

En dicho veredicto, en primer lugar, se pone de manifiesto que el ordenamiento procesal de la provincia de Buenos Aires, no requiere –bajo pena de nulidad– la orden del juez para obtener el listado de llamadas registradas por una línea telefónica, a diferencia de lo que ocurre con la interceptación de las comunicaciones para impedirlas o conocerlas (art. 229 del CPP).

Por el mismo camino, se evidencia en el precedente que, si bien la Ley Nacional de Telecomunicaciones 19.798 establece que la inviolabilidad de la correspondencia de las comunicaciones comprende tanto la "existencia" como el "contenido", hace una diferenciación entre la autoridad que puede disponer la intervención de una comunicación, y aquella facultada para obtener los registros de tráfico de una línea telefónica.

En el caso de la intervención de su contenido, el art. 18 ordena que sólo procederá a requerimiento de juez competente, mientras que al referirse a los registros de tráfico de comunicaciones (existencia) dispone que los prestadores del servicio deberán sistematizar tal información para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público, conforme el art. 45 ter incorporado por la ley 25.873 (Tribunal de la Casación Penal de la Provincia de Buenos Aires, causa número 68962 "L.M.A s/Recurso de Casación", voto del Dr. Carral, págs. 4-6).

En relación a la influencia que este tipo de tecnología posee en la esfera privada, Diego Fernández especifica que los datos que se pueden recolectar a través de dispositivos móviles resultan extremadamente valiosos en el marco de las investigaciones judiciales, sobre todo en el marco de investigaciones y juicios penales. Pueden ayudar a establecer que un

determinado sospechoso se encontraba en el lugar donde se cometió un delito mientras este sucedía y, por tanto, resulta razonable que las autoridades tengan un interés válido en querer acceder a estos datos. En tales casos, la cuestión radica entonces en determinar cómo debe balancearse el derecho a la privacidad de los individuos frente al acceso de las autoridades a sus datos y qué resulta razonable exigir para que este acceso sea legítimo. La privacidad es el derecho que todas las personas tienen a ser dejadas solas, sin intromisión de terceros, incluyendo al Estado, sin su voluntad y consentimiento. Por supuesto, este derecho no es absoluto y existen supuestos en los que otros derechos priman sobre el derecho individual a la privacidad (Fernández, 2023, p. 816).

Habiéndose puesto en discusión cuales son los requisitos para obtener la información que será objeto del análisis de las comunicaciones, como especie de la evidencia digital, debemos aclarar que en esta oportunidad no nos centraremos en lo que generalmente acaece en un estadio más avanzado de la investigación, esto es las escuchas telefónicas (contenido). En este caso, el quid de la cuestión versará sobre el análisis de los registros (existencia) respecto de llamadas entrantes y salientes, informes GPRS o megadatos, apertura de celdas e impactos de abonados en IMEI, entre otras cuestiones.

Es importante enmarcar el objeto de estudio del análisis de las comunicaciones, pudiendo precisar que los movimientos de telecomunicaciones resultan de interés en materia de investigación criminal en razón de tres puntos de estudio. En primer lugar, el relacional, en referencia a la vinculación los abonados entre sí. En segundo término, el espacial, tendiente a la geolocalización de comunicaciones mediante el impacto en celdas telefónicas, Por último, el temporal, en pos del examen de las variables dinámicas de las comunicaciones como ser fecha y hora o duración (Martínez, 2020, p. 6).

Como se observará en lo subsiguiente, toda esa información aporta una herramienta inconmensurable para las investigaciones penales. Pero antes de dar paso al método de investigación aquí propuesto, debemos definir a continuación algunos conceptos básicos para poder proseguir:

1) *Número de abonado*: es el número asignado desde el cual se emiten las comunicaciones (Enacom, 2011).
2) *Nro. de IMEI*: es el número que identifica al equipo de telefonía celular, siempre consta de 15 número, pero los 14 primeros son los que identifican al equipo, y el último es asignado por la compañía prestataria (Enacom, 2016).
3) *Celdas*: la celda es el espacio de cobertura de una antena de telefonía celular. Las compañías telefónicas tienen conocimiento de la ubicación exacta de las antenas, identifican el lugar donde se sitúan en función de variables de latitud y longitud. Por lo tanto, para el estudio de si el usuario de un abonado se encontró en determinado lugar será de interés: 1) lugar certero donde se ubica la antena, 2) radio de cobertura de la misma, 3) Azimut (Enacom, 2018).
4) *Azimut*: el radio de cobertura de una antena puede ser dividido en tres líneas a las que denominan Azimut. Las Azimut cortan los sectores a la mitad. De este modo, conociendo la ubicación de cada Azimut respecto del Norte (grado 0) quedan definidos los tres sectores de la antena. Esto permitirá reducir la zona de interés del radio de cobertura en pos de establecer si el usuario de un teléfono

se encontró o no dentro de una zona de interés para la investigación (Enacom, 2019).

5) *Megadatos o datos GPRS*: es una tecnología de datos para redes de telefonía móvil que permite enviar y recibir paquetes de datos de manera eficiente, siendo que cada registro del mismo brindará el impacto en una celda y permitirá determinar las diferentes ubicaciones de un abonado a lo largo de un período de tiempo (Enacom, 2017).

Para finalizar el acápite, corresponde determinar en coincidencia con lo expuesto por Martínez (2020, p. 36), que la tercera fuente de recolección, la central de nuestro trabajo, es la información asociada brindada por las empresas prestatarias de servicios de telecomunicación (la primera sería a través de las escuchas telefónicas, y segunda con el secuestro del aparato celular a través del examen mediante software UFED[1]).

Como veremos con más detalle, en breve se podrá solicitar información a las empresas prestatarias desde diferentes puntos de partida: 1) tráfico a partir de abonado, informando las prestatarias los registros de comunicaciones entrantes y salientes correspondientes; 2) tráfico a partir de celda, determinando una zona de interés y la prestataria devuelve los registros de comunicaciones entrantes y salientes de aquellas antenas, como también el impacto de megadatos o GPRS en dichas antenas; 3) tráfico de IMEI, cuándo se le brinda la numeración unívoca de un dispositivo a la prestataria y ésta aporta cuáles abonados (tarjetas SIM) impactaron en el dispositivo en cuestión.

3. La importancia de la utilización de un método

Como hemos venido desarrollando, la evidencia digital y en particular el análisis de las comunicaciones posee un bagaje técnico que complejiza su entendimiento. Por ello, el desarrollo de un método resulta fundamental no solo para no incurrir en errores a la hora de analizar los datos que aportan las compañías prestatarias de los servicios de comunicación, sino también para su publicidad y comprensión por la sociedad en su conjunto.

La dogmática penal ha desarrollado y estudiado por cientos de años un sistema o método lógico para establecer si una conducta específica constituye delito, esto es, una serie de niveles de análisis (acción típica, antijurídica y culpable) por los cuales el caso debe transitar para llegar a la conclusión de que existe delito (Hilgendorf y Valerius, 2017, p. 49; Rafecas, 2021, 177-185; Tarrío, 2015, 139-149). Este mismo sistema puede replicarse al tema aquí traído a análisis, a través del diseño de una serie de pasos que permita a cualquier interviniente o analista sacar diferentes conclusiones investigativas, pero a su vez que, al responder al mismo método investigativo, el proceso de acceso a las inferencias será conocido y comprendido por todos.

[1] UFED (Universal Forensic Extraction Device) es una herramienta desarrollada por la empresa Cellebrite, utilizada para la extracción, decodificación, análisis y presentación de datos digitales provenientes de dispositivos móviles. Esta tecnología permite recuperar información de teléfonos celulares y tarjetas SIM, incluso en casos donde los datos han sido eliminados o el acceso está restringido por bloqueos de seguridad. Información extraída de https://cellebrite.com.

En tal sentido, conforme la Real Academia Española, un método es un modo de decir o hacer con orden, pudiéndose referir también a un modo de obrar o proceder. Lo que aquí se propicia es un modo de hacer ordenado, mediante pasos lógicos que permitan sacar y evaluar conclusiones. Sentado ello, proponemos el estudio y aplicación de un método de examen de las comunicaciones de forma manual, claro y sencillo que pueda ser desarrollado por cualquier operador o analista con instrucción en la materia y entendido al ser explicado por estos por el resto de las personas.

Este método consiste en su inicio de cuatro simples pasos. Se parte solapadamente de una investigación en la cual las medidas de investigación convencionales en las primeras fases de la pesquisa han fallado, presuponiendo que en el hecho criminal investigado existe la sustracción de un teléfono celular. Ello no obedece a una cuestión de animosidad o ceguera, sino que pone al analista ante un panorama más complejo; el resto no ha funcionado y la sola investigación del equipo sustraído puede brindar diversas soluciones a la difícil situación en la que se encuentra el detective. Ahora bien, veremos también que, si se cuenta con información de los posibles involucrados en los hechos y sus posibles números de telefonía celular, el método podrá comenzar en un paso más avanzado resultando innecesario el inicio a través de los primeros pasos. Así también, en caso de no haber un equipo sustraído la investigación podrá comenzar en pasos subsiguientes con la información obtenida de otros métodos pesquisantes.

Como segunda advertencia, debemos decir que el camino de este método contará en todos sus pasos con una triple vertiente de ejecución, solicitud de información, recepción y análisis de dicha información, informe de lo analizado. Producido el triple canal de estudio, se continuará al siguiente paso de la misma forma: solicitud, análisis, informe.

Por último, en general en los procesos acusatorios mixtos y tal como se ha explicado *supra*, consideramos que la solicitud estará en cabeza del Ministerio Público Fiscal y podrá hacerlo directamente ante las empresas prestatarias, mediante oficio o portal de información, o bien, estableciendo como canal de diálogo entre el organismo judicial y las empresas a la DAJUDECO[2]. Ejemplificaremos, como hemos advertido, a través del inicio de una investigación penal preparatoria en donde supondremos además que en el hecho delictivo se apoderaron ilegítimamente de al menos un teléfono celular.

Paso número 1:

Punto 1: Como primera medida, se solicitará a las empresas prestatarias de servicios de telefonía que informen, en base al número de línea del teléfono sustraído (obtención mediante testigos o sistemas de información), el listado de llamadas entrantes y salientes del abonado desde quince días antes de hecho hasta el día de la solicitud.

Como en cualquier otra medida de investigación, dicho paso posee una lógica de indagación criminal, que no es ni más ni menos que obtener el nro. de IMEI del equipo sustraído. Por ello, si se cuenta con ese dato previamente a través de la caja del teléfono celular o mediante alguna situación análoga, dicho punto del paso 1 no será necesario a menos que

[2] Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado dependiente de la Corte Suprema de Justicia de la Nación, única dependencia estatal autorizada para realizar escuchas telefónicas legales y además funciona como enlace entre las autoridades judiciales y las empresas prestatarias a través de la sección información asociada de dicha dependencia.

se quiera contar previamente con un patrón de frecuencia comunicacional de la víctima en pos de establecer un posible móvil del hecho criminal investigado.

Punto 2: A su vez, se solicitará se informe el impacto y activación de megadatos o informe GPRS de dicho abonado, desde el día anterior al hecho hasta el día posterior. En este caso, el motivo de la solicitud tiene como objetivo investigativo evaluar el posible recorrido del teléfono sustraído luego del hecho –y por tanto de los incusos– si es que no lo apagaron a posterior del despojo, y de esta manera establecer el posible camino de huida de los imputados.

La solicitud abarca el día anterior al hecho, para establecer un patrón de frecuencia de antenas, es decir qué antenas son las habituales del usuario del teléfono sustraído para su posterior comparación; y del día posterior a fin de poder conocer si el aparato tuvo un período de "enfriamiento" para ser puesto en funcionamiento en las horas siguiente y determinar en qué lugar.

Paso número 2:

Luego de haber solicitado, analizado y realizado un informe a partir de la información descripta en el paso 1, se continuará con el paso nro. 2. Antes de emitir una nueva solicitud, se debe comprobar si el nro. de IMEI se corresponde con el equipo sustraído, para lo cual podemos recurrir a algunas páginas públicas[3] con el objeto de constatar si el IMEI emergente del análisis de las comunicaciones se corresponde con el modelo informado por la víctima o sus familiares.

Verificada tal situación, en el paso nro. 2 se solicitará a todas las empresas de telefonía celular que informen si nuevos abonados telefónicos han impactado con posterioridad al ilícito investigado en el equipo sustraído (IMEI). Es importante aclarar que la solicitud no sólo será ante la empresa que brindaba servicio telefónico a la víctima, sino a todas las compañías. Ello en función a que el teléfono se puede encontrar "liberado", es decir apto para su utilización en cualquier empresa de telefonía o puede ser "liberado" con posterioridad al hecho. El objetivo de este paso es determinar si, con posterioridad al hecho, el celular sustraído fue puesto en uso al colocarle un nuevo chip y, por tanto, encontrarse funcionando con otro nro. de abonado. Uno podría preguntarse cuál fue la utilidad del paso 1, punto 2. El recorrido del abonado de la víctima puede permitir orientar otras medidas investigativas, como por ejemplo el relevamiento de cámaras. Será de utilidad, además, en los pasos subsiguientes para el cotejo de celdas con los teléfonos de presuntos imputados.

Paso número 3:

De aquí en adelante, la solicitud será idéntica a la del paso nro. 1 pero mutando la variable de análisis. En este caso, la variable en estudio no será el abonado telefónico de la víctima sino aquel que haya emergido en una *check list* positiva de empresas prestatarias del paso nro. 2. Es decir, aquel abonado que haya sido inserto en el teléfono celular sustraído a la víctima.

[3] Por ejemplo: https://imeicheck.com/es/verificador-imei.

Si la lista de control del paso nro. 2 ha arrojado resultado negativo en cuanto a nuevos impactos, en esta faceta de investigación de las comunicaciones se produce un corte en el camino y deberá trabajarse con otras variables comunicacionales, como ser impactos coincidentes en registros de antenas de interés, tema este que excede el objeto de este artículo. Asimismo, se puede recurrir a otras fuentes de pesquisa para poder partir con el teléfono de un imputado identificado desde este mismo punto. En este último caso, o bien si el paso nro. 2 ha arrojado resultado positivo, se deberá proceder de la siguiente manera:

Punto 1: Utilizando como variable el teléfono del presunto imputado o aquel que impactara en el IMEI que se corresponde con el equipo sustraído, se solicitarán llamadas entrantes y salientes desde 15 días antes del hecho hasta el momento de la solicitud. Ello tiene como objetivo crear un patrón de frecuencia comunicacional del imputado que, a la postre, será de utilidad en el paso nro. 4. Además, se deberán prestar especial atención a las llamadas que realice el usuario el día del hecho, así como el día anterior y posterior.

Punto 2: Quizás este sea el punto más importante del método explicado. Se solicitará del teléfono del sindicado o de aquel que impactara en el celular sustraído, informe de GPRS desde el día anterior al hecho hasta el día posterior. Lo que se busca, principalmente, con este pedido de información y análisis, es determinar la ubicación del teléfono celular del sindicado en el momento en que se estaba cometiendo el hecho investigado, pero también su movimiento antes y después del evento. Se deberá tener en cuenta, entre otras cuestiones, si con posterioridad al hecho su impacto de antenas resulta coincidente con el del abonado de la víctima extraído del paso 1 punto 2.

Es cierto que la geolocalización por este medio no dirá con exactitud la ubicación del usuario. Y, para mayor precisión, deberán estudiarse cuasi escalonadamente la ubicación de la antena, radio de cobertura, Azimut, tiempo de arribo de la señal[4] y sectorización[5]. Sin perjuicio de ello, el estudio de este punto indicará un fuerte indicio de reprochabilidad en determinadas circunstancias. Tal es así que, si la persona imputada reside a unos cuantos kilómetros de distancia del lugar del hecho, pero gracias a los datos GPRS es posible ubicar el trayecto del teléfono desde cercanías de su domicilio hasta el lugar de comisión del injusto y luego volver a proyectar su recorrido hacia su lugar de residencia, esto importará un indicio probatorio de suma relevancia, todo lo que podrá ser plasmado en un mapa interactivo (por ejemplo, mediante la aplicación de Google Maps) que a la postre servirá didácticamente en la explicación ante la judicatura.

Debemos tener en cuenta que cada notificación, cada interacción que tenga el usuario del teléfono por medio de alguna aplicación como ser una red social (WhatsApp, Instagram, Facebook, etcétera) genera un impacto de datos GPRS, el cual se registrará en una antena cercana a la ubicación física del aparato.

Es gracias a ello que podemos trazar, luego de analizar la información, el recorrido de ese teléfono celular, e incluso podemos ubicarlo con mayor precisión si las compañías nos

[4] La estimación del tiempo de llegada TOA por sus siglas en inglés (Time of Arrival) es una técnica de posicionamiento que permite medir la distancia, estableciendo así la ubicación. En este caso y sin perjuicio de que excede el eje del presente se tendrá en cuenta los factores tiempo distancia entre la ubicación de la celda y el teléfono celular.

[5] La sectorización de la DAJUDECO permite visualizar en un mapa interactivo la zona aproximada de cobertura de cada celda utilizada por el abonado objeto de investigación. Visto en: www.mpfchubut.gov.ar/images/pdf/Resoluciones/2022/RES091-E_Anexo_DAJuDeCO.pdf.

proporcionan los datos requeridos de radio de cobertura y Azimut. Con ello, se adquirirá precisión en referencia al rango, forma y dirección de apertura, sin perjuicio de lo cual existen otros estudios para precisar más la cuestión.

Por último, si de este paso se obtuvieron resultados positivos, tanto sea que mediante llamadas o impactos de GPRS, habremos podido ubicar el teléfono que venimos analizando en cercanías al lugar del hecho al momento de su comisión, y por lo tanto arribar a algunas conclusiones parciales. Veamos.

El usuario de ese abonado, con la probabilidad que requiere la instancia, participó del hecho investigado. Ahora bien, es importante acreditar que el titular de dicho abonado es el usuario del teléfono. Así, para dar con su verdadera identidad es recomendable agregar el número a la aplicación WhatsApp para poder obtener su fotografía y *nickname* de aplicación y ver si coinciden con la titularidad o bien extraer su fotografía y mandar a cotejar al sistema de individualización criminal de Policía Federal. Otra herramienta útil es la simulación de una transferencia a través de la aplicación de Mercado Pago. En la Provincia de Buenos Aires también contamos con la aplicación cuenta DNI, que resulta ser similar a Mercado Pago, por lo que también se puede en ese caso realizar una simulación, considerando que ambos sistemas poseen requisitos de ingreso biométricos que hacen presumir que el usuario de la aplicación es el portador del abonado. Estas son algunas de las opciones, las más básicas y comunes en este tipo de investigaciones. Pero cada investigación posee diferentes desafíos, por lo que cada una de ellas nos va a llevar a adoptar distintas acciones.

Paso número 4:

Punto 1: Tal como hemos adelantado, desde el paso nro. 3 en adelante siempre se vuelve a realizar la misma solicitud de información, pero cambiando la variable de análisis. En el caso de este punto, se solicitarán llamadas entrantes y salientes desde 15 días antes del hecho de todos los abonados obtenidos en el punto 1 del paso 3 (patrón de frecuencia comunicacional del abonado obtenido en el paso nro. 2 o del presunto abonado de un imputado). Es decir, en el paso nro. 3 punto 1 se obtienen aquellos abonados con los cuales se comunica frecuentemente el teléfono de interés. Se pueden elegir los cinco, diez, quince o más teléfonos frecuentes, dependiendo de la gravedad de la investigación. Esto tiene como objetivo investigativo formar un patrón de frecuencia comunicacional de cada número en pesquisa ahora.

Punto 2: Respecto de todos los números obtenidos en el paso nro. 3 punto 1, se analizará su impacto de GPRS a fin de determinar si pueden ser ubicados en el lugar de los hechos o si presentan coincidencia de impactos con el abonado de la víctima, o bien con el del abonado que impactara en el celular sustraído o con el abonado identificado de un investigado. También permitirá acreditar si los usuarios de los abonados ahora en estudio pueden o no tener relación con el hecho investigado. Respecto a aquellos abonados de los cuales se obtenga un resultado positivo, deberá volverse al punto anterior (paso 4 punto 1), ver su frecuencia comunicacional y obtener aquellos abonados de utilidad para comenzar con la solicitud del paso nro. 5, y así sucesivamente dependiendo la cantidad de involucrados en el evento criminal.

4. Conclusión

A lo largo del presente hemos brindado una aproximación acerca de la importancia del avance de las nuevas tecnologías no solo en la vida cotidiana sino también en referencia a su injerencia en el Derecho Penal y por sobre todo en la investigación criminal. Entendemos que la comprensión del análisis de las comunicaciones resulta fundamental para propiciar investigaciones de calidad y poder así brindar un correcto servicio de justicia. En tal sentido, dimos a conocer que la formulación de un método de análisis permite no solo dotar de previsibilidad y seguridad a sus conclusiones sino también de entendimiento para los propios analistas, los operadores judiciales y la sociedad en su conjunto.

Como resultado de ello, hemos sentado que el método explica el caso, permite emitir conclusiones, formular y descartar hipótesis, pero que también el caso explica el método, desde la situación de hecho traída a conocimiento se logra una mejor comprensión de esta serie de pasos lógicos, que vaya paradoja fue creada para explicar los casos.

Poseemos la firme convicción de que este es solo un inicio, una forma de comunicar nuestra manera de entender el análisis de las comunicaciones, que puede ser robustecida, criticada, mejorada, alterada o bien sustituida por ideas superadoras, y que todo ello contribuirá en seguir avanzando hacia un sistema, lógico y complejo, pero previsible y entendible, de investigación criminal en base al examen de las comunicaciones. Dicho sea de paso, consideramos que no hay margen de dudas de que su explicación resulta ser la mejor manera para que tanto los operadores judiciales como la sociedad puedan entender de qué se trata.

Referencias

ENACOM (2011). *Plan Fundamental de Numeración Nacional*, "Anexo III – Definiciones", Buenos Aires.

ENACOM (2016). Resolución 2459/2016, "Procedimiento para el bloqueo de terminales con reporte de robo, hurto o extravío y la identificación de IMEI irregulares".

ENACOM (2017). *Manual de conceptos básicos de telecomunicaciones y servicios móviles*, Buenos Aires.

ENACOM (2018). "Radiobases para Servicios de Comunicaciones Móviles".

ENACOM (2019). "Parámetros técnicos para antenas de radiobases".

Fernández, Diego (2023). "Análisis doctrinal y Jurisprudencial", Tomo I, en: Torres, Sergio G. y Basílico, Ricardo A. (directores), 2023. *Código Procesal Penal de la Provincia de Buenos Aires*. Hammurabi, Buenos Aires.

Hilgendorf, Eric, Valerius, Brian (2017). *Derecho Penal.* "Parte General". AD-HOC, Buenos Aires.

Lorenzo, Leticia (2014). *Manual de Litigación*, Ediciones Didot, Buenos Aires.

Martínez, Alejandro M. (2020). "Análisis de redes, comunicaciones telefónicas e investigación penal", Repositorio institucional digital de acceso abierto de la Universidad de Quilmes, Buenos Aires.

Ministerio de Seguridad de la Nación (2023) "Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital". Visto en: https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf

Ministerio Público Fiscal de la Ciudad autónoma de Buenos Aires (2013). "Protocolo de gestión de almacenamiento de la evidencia digital", disponible en:

https://documentosboletinoficial.buenosaires.gob.ar/publico/PJ-RES-MPF-FG-107-23-ANX.pdf

Rafecas, Daniel (2021). *Derecho penal sobre bases constitucionales*. Ediciones Didot, Buenos Aires.

Tarrío, Mario C., Tarrío, Gonzalo A. (2015). *Manual de Derecho Penal*. "Parte General", Cathedra Jurídica, Buenos Aires.