LA UTILIDAD DE LOS DATOS DE GEOLOCALIZACIÓN EN LA ESTRATEGIA DE DEFENSA. ANÁLISIS DE UN CASO[1]

Antonella M. Bentín[2]

1. INTRODUCCIÓN

La evolución de las TIC le ofrece al Estado una serie de ventajas que compensan o —según algunos— incluso superan las desventajas derivadas de la creciente dificultad en el acceso al contenido de las comunicaciones debido a los métodos de encriptación existentes. Así, cada vez más autores sostienen que no solo no es cierto que el Estado se esté "quedando a oscuras", sino que, en realidad, estamos ingresando en la "edad de oro de la vigilancia" (Blanco, 2020, p. 249).

Este avance tecnológico, que es cada vez mayor, ha impactado en las investigaciones penales ya que la información que los individuos otorgamos de manera "voluntaria" a terceros (como empresas prestatarias de telefonía, internet, plataformas digitales, etc.) muchas veces sirve como prueba para poder llegar a vincular —o no— a alguien en un hecho delictivo en concreto.

Asimismo, respecto al contenido que se puede extraer de un dispositivo, los datos de geolocalización se han convertido en una herramienta indispensable en las investigaciones penales, ya que ofrecen información relevante sobre los movimientos y la ubicación de los dispositivos móviles. Este avance tecnológico proporciona a los investigadores la capacidad de reconstruir escenas del crimen, establecer cronologías y verificar coartadas con un nivel de precisión antes inalcanzable.

Si bien los datos de geolocalización que contiene un dispositivo celular pueden ser de suma utilidad para el marco de una investigación, esta información se encuentra amparada por el derecho a la privacidad debido a la vigilancia enciclopédica y perfecta que se genera con dichos datos a lo largo del tiempo[3]. Es la autoridad judicial quien debe fundamentar la necesidad de esa medida (ya sea solicitar a una empresa privada la información o proceder a la extracción forense del contenido del dispositivo), y también que esta sea proporcional e idónea respecto al delito que se encuentran investigando.

Los datos de geolocalización en las investigaciones criminales no están exentos de desafíos y riesgos. A pesar de su gran utilidad, la confianza en estos datos debe analizarse con cautela ya que por sí solos pueden no llegar a proporcionar información concluyente. Por ello, es importante comprender tanto las fortalezas como las limitaciones de los datos de geolocalización y verificar que estos se corroboren adecuadamente con otras pruebas, lo que resulta esencial para mantener una hipótesis acusatoria o defensiva.

La interpretación errónea de los datos de ubicación o su uso sin otras pruebas que los corroboren puede llevar a conclusiones incorrectas. En ese sentido, es importante que

[1] Cítese como Bentín, A. 2025. La utilidad de los datos de geolocalización en la estrategia de defensa. Análisis de un caso, Estudios de jurisprudencia, 189-202.

[2] Abogada. Especialista en Derecho Penal (UP). Especialista en Cibercrimen y Evidencia Digital (UBA). Funcionaria del Ministerio Público de la Defensa.

[3] Corte Suprema de Justicia de Estados Unidos, "Carpenter v. United States", 585 U.S., resuelto el 22/06/2018. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/5253.

como defensa realicemos un examen autónomo e independiente de las conclusiones a las que haya arribado el perito informático auxiliar de la justicia, a fin de controlar y evaluar los datos obtenidos. Esto permitirá diagramar posibles estrategias de defensa o analizar si esos datos pueden ser de interés para probar nuestra teoría del caso.

Es así como, en el marco del presente trabajo, analizaré un fallo —sobre un caso en concreto que asistimos dentro de la Defensoría—, en el que logramos probar nuestra hipótesis a través de los datos de geolocalización que se extrajeron de un dispositivo celular, los que —como adelanté— se analizaron en conjunto con otras medidas de pruebas.

Para abordar esta problemática, este trabajo se divide en tres apartados. En primer lugar, se resalta la relación entre el derecho a la intimidad, las medidas de injerencia estatales y el principio de proporcionalidad. Asimismo, se expone un análisis de las características específicas de la evidencia digital, con foco en los protocolos de recolección, la cadena de custodia y los marcos normativos que regulan su tratamiento, con especial atención a la geolocalización como elemento probatorio. En segundo término, se presenta un caso concreto, en el cual los datos de geolocalización resultaron determinantes para el sobreseimiento del imputado. Por último, se formulan conclusiones orientadas a identificar las mejores prácticas para el uso estratégico de esta evidencia desde el ejercicio de la defensa.

2. DERECHO A LA INTIMIDAD VS. MEDIDAS DE INJERENCIA. PRINCIPIO DE PROPORCIONALIDAD, RAZONABILIDAD E IDONEIDAD

En comparación con épocas anteriores las capacidades de vigilancia se han expandido considerablemente, ya que el Estado cuenta con una capacidad nunca vista. Ejemplo de ello es la información sobre la localización y la proliferación de bases de datos que generan “ficheros digitales” sobre la vida de las personas (Center for Democracy and Technology, 2011).

Por otro lado, no solo el Estado y las empresas privadas recopilan datos, sino que también existe una gran cantidad de información que almacenan los dispositivos electrónicos sobre nuestra vida personal. La teoría del mosaico consiste en que pequeños datos de una persona —en este caso la geolocalización—, pueden reflejar gran información de la vida privada, como los lugares a donde va semanalmente, gustos, preferencias sexuales, religiosas, etc., lo que fue analizado en el precedente “Carpenter”[4].

En el mismo sentido, otros precedentes jurisprudenciales[5] también resaltan la injerencia en la intimidad que se puede generar con la obtención de los datos de geolocalización de

[4] La jueza Sotomayor sostuvo que “mapear la ubicación de un teléfono celular durante el curso de 127 días proporciona un registro completo del paradero del titular. Al igual que con la información del GPS, los datos con marca de tiempo proporcionan una ventana íntima a la vida, revelando no solo sus movimientos particulares, sino a través de ellos sus "asociaciones familiares, políticas, profesionales, religiosas y sexuales”. Entonces, “un teléfono celular sigue fielmente a su dueño más allá de las vías públicas y hacia residencias privadas, consultorios médicos, sede política. En consecuencia, cuando el Gobierno rastrea la ubicación de un teléfono celular logra una vigilancia perfecta, como si hubiera conectado un monitor de tobillo al usuario del teléfono”.

[5] Véase Corte Suprema de Estados Unidos, “United States v. Jones”, 565 U.S. 400, resuelto el 23/01/2012, disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/5252 y Tribunal Europeo de

un individuo en particular, los que han sido analizados en el boletín "Evidencia Digital y Derechos Humanos" publicado por el MPD en coautoría con ODIA (2023)[6].

Ahora bien, la manera más eficiente de obtener los datos que generan y almacenan los dispositivos, es a través de su secuestro y posterior peritaje informático. Es importante destacar que es la autoridad judicial quien debe fundamentar la necesidad de esa medida de injerencia, como así también tiene que ser proporcional e idónea respecto al delito que se encuentran investigando.

Para profundizar en esta cuestión, la intervención judicial debe basarse en criterios estrictos de proporcionalidad que evalúen la gravedad del delito investigado frente a la afectación a la intimidad que implica el acceso al contenido de un dispositivo móvil.

En principio, no resultaría proporcional, por ejemplo, intervenir una línea telefónica si se está investigando un delito de lesiones leves. Con base en este razonamiento, tampoco sería razonable secuestrar y realizar una extracción de toda la información de un teléfono celular —que contiene más contenido que una simple llamada telefónica— cuando se investigan delitos que pueden probarse por otros medios menos lesivos de los derechos fundamentales (Bentín, 2024, p. 122).

La información que sea incorporada a la causa debe ser relevante (cfr. uno de los principios de las normas ISO/IEC 27037:2012) ya que solo corresponde que sean tenidos en cuenta aquellos elementos que son significativos a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y debe ser excluido del material probatorio[7]. En el mismo sentido, la defensa debe ofrecer puntos de pericia que crea que puedan coadyuvar a su estrategia de defensa.

Tal como lo afirma la Asociación por los Derechos Civiles (2021)

> esto genera desafíos sobre cómo deben realizarse las órdenes de secuestro y búsqueda de información en equipos electrónicos para evitar una potencial afectación al derecho a la privacidad. Las reglas tradicionales que regulan el allanamiento físico tampoco se ajustan de forma adecuada a la búsqueda de información en dispositivos digitales. Para atenuar la afectación a la intimidad que significa el acceso a un celular, las autoridades deberían procurar que el análisis de la información se encuentre limitado por el objeto de investigación que motivó la medida (p. 23)

En torno a las órdenes de búsqueda que son demasiado "genéricas", en el boletín de jurisprudencia del MPD ya mencionado, también se recopilaron fallos en los que se aborda esta problemática: se han limitado las búsquedas que resultaban excesivas por excederse del objeto de investigación o no tener una delimitación temporal.

Derechos Humanos, "Ben Faiza v. Francia", Aplicación N° 31446/12, resuelto el 08/05/2018. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/5255.

[6] Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/5342.

[7] Al respecto, puede consultarse Universidad FASTA & Universidad Champagnat (2022).

En ese sentido, me interesa poner de resalto el precedente de la Suprema Corte de Georgia en el caso "The State v. Wilson"[8], que confirmó la decisión que hizo lugar a la moción presentada por el imputado para suprimir la orden que autorizó un examen forense de su teléfono celular, por resultar demasiado amplia. En ese caso, un juez, a pedido de los investigadores, había emitido una orden para llevar a cabo un examen forense del teléfono celular del imputado, quien era acusado de asesinato[9], para obtener "cualquier y toda la información electrónica almacenada, incluyendo pero no limitado a información de la cuenta de usuario, información almacenada del teléfono, imágenes, mensajes de texto, videos, documentos, correos electrónicos, actividad de Internet, registros de llamadas, información de contacto, información de la guía telefónica o cualquier dato eliminado".

El acusado cuestionó la validez de la orden para realizar el examen forense sobre el teléfono e hizo un planteo para excluir la información que se obtuvo. El juez de tribunal oral hizo lugar al planteó y explicó con suma claridad que esa orden era demasiado amplia y que se había autorizado una búsqueda general de los datos personales de Wilson sin causa probable en violación de la Cuarta Enmienda.

La Suprema Corte de Georgia confirmó la decisión que había hecho lugar al pedido de la defensa de Wilson. El juez Peterson en su voto concurrente señaló que: "el problema que plantea la orden general no es el de intrusión per se, sino de un hurgar general y exploratorio en las pertenencias de la persona". Asimismo, expresó que una orden de buscar y apoderarse de "cualquiera y todos los datos almacenados en un teléfono celular", ni siquiera limitado a la evidencia del delito en cuestión, sin especificidad sobre cómo se podría usar cualquiera de los datos, viola la Cuarta Enmienda.

Por su parte, el juez Pinson, en su voto concurrente, explicó que los teléfonos celulares no son de hecho casas, pero después del caso "Riley"[10], no está claro por qué los teléfonos celulares no deberían ser tratados en modo parecido. De lo contrario, con la lógica genérica de "los delincuentes también usan teléfonos celulares", sería difícil imaginar un caso en el que la policía no pueda obtener la orden que autorice el examen.

La sentencia finaliza reflexionando que el punto es concreto: "Riley hizo inequívocamente claro que cuando se trata de aplicar la Cuarta Enmienda, los teléfonos móviles modernos no son un objeto físico más" (p. 40) .

---

[8] Corte Suprema de Georgia, "The State v. Wilson", S22A0967. Disponible en https://www.gasupreme.us/wp-content/uploads/2023/02/s22a0967.pdf.

[9] El 28 de enero de 2021, Bradly Jordan fue asesinado a tiros mientras realizaba servicios de control de plagas en un complejo de apartamentos. Después de realizar una investigación en la escena del crimen, los oficiales determinaron que el tirador era un "hombre negro" conduciendo una "Furgoneta Ford Aerostar modelo [1990] verde azulado". Utilizando un sistema de rastreo de matrículas, los oficiales localizaron una camioneta que coincidía con esta descripción a pocos kilómetros del incidente. Wilson figuraba como el propietario registrado del vehículo. La policía detuvo el automóvil y habló con Wilson, quien conducía el auto. Después de contestar algunas preguntas Wilson fue arrestado, y su vehículo incautado. Luego de obtener una orden, la policía registró el vehículo y encontró dos teléfonos celulares que pertenecían a Wilson.

[10] Corte Suprema de Justicia de Estados Unidos, "Riley v. California", 573 U.S. 373, resuelto el 25/06/2014. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/2572.

Además, "Este caso ilustra un problema que surge luego de la decisión ´Riley´. Este consiste en que, por el simple hecho de que exista un teléfono celular durante el curso de una investigación, se supone que hay causa probable para examinar su contenido" (p. 42), situación que es desacertada y la vemos de manera repetida en nuestro ordenamiento jurídico[11].

Como conclusión parcial, es importante comprender que al momento de ordenar una medida intrusiva como es el secuestro y posterior pericia de un dispositivo, se debe establecer con claridad cuál es el objeto de investigación como así también limitar esa búsqueda a un periodo temporal determinado (días o meses), a fin de que la intimidad de la persona se vea afectada lo menos posible.

3. CARACTERÍSTICAS DE LA EVIDENCIA DIGITAL. PROTOCOLOS Y GUÍAS DE BUENAS PRÁCTICAS

Para adentrarnos en la parte de recolección, extracción y análisis de evidencia digital, primero resulta importante comprender las características que distinguen a la evidencia digital de la evidencia física. Tal como lo explica Sueiro (2019), "el secuestro de un efecto físico, corpóreo, material o tangible [...] requiere de mecanismos de preservación [...] muy distintos a los de la preservación de un dispositivo electrónico" (p. 47).

En el mismo sentido, la "Guía de Recomendaciones para la Implementación de Protocolos de Actuación para la Adquisición, Preservación y Presentación de la Prueba Digital –PAFE– CCyLF" (Universidad FASTA & Universidad Champagnat, 2022), explica que una de las características principales de la evidencia digital y que la torna compleja en sí misma, es su volatilidad. Ello conlleva a que, por su propia naturaleza, sea frágil, fácil de alterar y dañar o directamente de destruir. Asimismo, en la guía de recomendación se sostiene que la metodología que se utilice para la identificación, recolección, obtención y preservación de la información resultará crucial a fin de que la evidencia digital pueda ser utilizada con eficacia en el proceso judicial.

La evidencia digital es cada vez más relevante en investigaciones judiciales, sin embargo, su valor probatorio depende directamente de su integridad, autenticidad y trazabilidad. Para garantizar esto, es fundamental que se respete la cadena de custodia, es decir, un registro documentado y continuo que detalle quién, cuándo, cómo y dónde accedió o manipuló los dispositivos electrónicos y la respectiva evidencia digital, desde su obtención hasta su presentación en juicio.

Dado que la evidencia digital es altamente volátil y fácilmente alterable, incluso de forma no intencional, deben emplearse herramientas forenses específicas como así también el personal debe ser idóneo y capacitado para su proceder a su manipulación.

Ante la ausencia de regulación procesal específica, a lo largo de los años, se ha ido creando distintos protocolos y guías de buenas prácticas respecto a cómo se debe recolectar y preservar la evidencia digital para garantizar su inalterabilidad y utilidad, los cuales veremos a continuación. Entre ellos pueden mencionarse normas ISO/IEC

[11] Véase análisis detallado en Bentín (2024, pp. 123-126).

27037:2012[12], el "Protocolo de actuación para pericias informáticas" de la provincia de Neuquén del año 2012, la "Guía de obtención, preservación y tratamiento de evidencia digital" (UFECI), el "Protocolo general de actuación para las fuerzas policiales y proceso de recolección de pruebas en ciberdelitos" (Resolución 234/2016) del Ministerio de Seguridad de la Nación.

Por último, en abril de 2023 se ha publicado en el Boletín Oficial el "Protocolo para la identificación, recolección, preservación, procesamiento y presentación de la evidencia digital" creado por el Ministerio de la Seguridad de la Nación, el cual resulta obligatorio para las fuerzas federales.

Dicho protocolo en el capítulo V, diferencia los distintos procedimientos que se deben llevar a cabo de manera específica según el tipo de dispositivo electrónico que se vaya a secuestrar (dispositivos celulares, computadoras de escritorio, laptop o computadora portátil, GPS, servidores, etc.)

De modo resumido, de acuerdo con ese protocolo, se deben transitar las siguientes etapas:

1.Identificación: se deben seleccionar qué elementos se secuestrarán, ya que al momento de realizar un procedimiento pueden hallarse dispositivos electrónicos que son de personas que no poseen calidad de imputadas, por lo tanto, se deberá dejar afuera todo aquello que no sea de utilidad para la investigación.

2.Recolección y preservación: filmar y detallar en un acta todo el material secuestrado: si los dispositivos móviles estaban apagados o encendidos, su estado de conservación, registrar la marca, modelo, números de la tarjeta SIM, etc. Se rotula y embala los dispositivos: de ser posible colocar el dispositivo en modo avión, en bolsas Faraday o envolver los dispositivos al menos tres o cuatro veces en papel aluminio. Luego deberán embalarse de manera cerrada, franjada y firmada por los testigos de procedimiento.

3.Adquisición y análisis: a través de herramientas forenses una persona con *expertise* en la materia, deberá extraer la información en un laboratorio forense y analizará el contenido que es útil conforme los puntos de pericia solicitados.

4.Presentación: Se elabora un informe pericial respecto a los puntos de pericias solicitados, explicando el procedimiento que se ha llevado a cabo.

Respecto al punto 3, resulta necesario resaltar que la gran mayoría de las herramientas y programas que las fuerzas de seguridad, las fiscalías y los auxiliares de justicia utilizan para extraer datos de dispositivos móviles son desarrolladas y vendidas por empresas del sector privado. Estas herramientas incluyen softwares que funcionan bajo lo que se conoce como Software Comercial o Privativo, es decir, que el código fuente de la herramienta se encuentra protegido por el derecho de propiedad intelectual y suele ser comercializado a título oneroso, como por ejemplo *Cellebrite*, *Oxygen Forensic Detective*, *Magnet Axiom*, *XRY*, *MobilEdit*, *GrayKey*, etc.

[12] ISO/IEC. (2012). ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.

Al momento de utilizar dichas herramientas para realizar la extracción del contenido que posee un dispositivo —como ya lo adelanté— se debe contar con *expertise* en la materia. El ejemplo más actual que denota lo necesaria que es la *expertise* —ya que la extracción de información de un teléfono celular se puede tornar irreproducible—, es el caso de Fernando Sabag Montiel, acusado de atentar contra la vida de la expresidente Cristina Fernández de Kirchner. En el marco de esas actuaciones, se convocó a la Policía Federal Argentina (PFA) para intentar hacer la extracción de información a través del software UFED en la sede del Juzgado. Al no poder realizarse la extracción, se envió el dispositivo a la sede de la PSA. Sin embargo, al momento de intentar realizar la extracción en la PSA, apareció un aviso que el teléfono estaba reseteado a estado de fábrica.

Actualmente la causa se encuentra en pleno debate oral y resulta de suma utilidad ver las audiencias que están disponibles para visualizarlas —en la plataforma *Youtube*—, donde las personas que intervinieron en el secuestro e intento de extracción del contenido del dispositivo, prestan declaración testimonial y explican las acciones que realizaron. Para destacar algunos puntos que llaman la atención es que, por ejemplo, la apertura y primer intento de extracción se realizó en la sede del Juzgado, cuando todos los protocolos indican que debe realizarse en un laboratorio forense, donde los dispositivos se encuentren aislados de cualquier tipo de señal o interferencia —entre otras recomendaciones—.

Independientemente de cuál es la explicación técnica que se debate en el juicio —es decir, si fue un fallo de la herramienta UFED por la configuración del teléfono, el cual con anterioridad había sido rooteado—, lo que viene a demostrar este caso es que la extracción con UFED tiene que ser realizado por personal calificado y su naturaleza es pericial (contrario a lo afirmado en el precedente "AJA y otros s/nulidad"[13]). Si la extracción no se realiza por personal calificado (*expertise*) y con las debidas diligencias del caso —ya que muchas veces la complejidad depende del dispositivo que se va a manipular— el dispositivo puede verse afectado y así frustrarse la extracción de evidencia digital.

Tal como lo indican los protocolos de actuación, cualquier acción que implique una alteración irreversible de la evidencia debe ser previamente informada al director de la investigación, a las autoridades judiciales y quedar debidamente documentada.

Es importante conocer el Protocolo y tenerlo en consideración, ya que no sólo sirve de guía para las fuerzas de seguridad al momento de recolectar y/o manipular la evidencia digital, sino también para que los operadores judiciales puedan advertir si hubo algún tipo de irregularidad en la manipulación de esta, que traiga como consecuencia un planteo de nulidad[14].

4. LA IMPORTANCIA DE LA CADENA DE CUSTODIA

[13] Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, Sala VI, "A.J.A. s/Nulidad", CCC 81978/2018/11/CA9, resuelto el 20/09/2019. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/3978.

[14] Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala VI, "G.F.J. s/ Nulidad", causa N° 37433/2018. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/1921.

Los procedimientos mencionados para la recolección de evidencia digital encuentran su fundamento jurídico en el concepto de cadena de custodia. Su importancia radica en que de su correcta ejecución depende la confiabilidad de la prueba, lo cual resulta determinante para su valoración en el proceso penal. Como lo señala Reale (2023), permite a la persona imputada auditar y controlar cada acción realizada sobre la evidencia por las personas intervinientes durante el proceso penal, y realizar las acciones judiciales necesarias para señalar tratamientos indebidos sobre la evidencia.

Por ende, el acusado tiene derecho a examinar y controlar la prueba producida y, en este punto, la cadena de custodia será, sin dudas, una herramienta valiosa para conocer las acciones que se realizaron. Como contracara, permitirá a las personas que intervinieron durante dicho proceso dejar constancia de que sus acciones se realizaron de manera adecuada y no alteraron la evidencia (Reale, 2023, p. 65).

El CPPF en el artículo 157 alude a la cadena de custodia estableciendo que "con el fin de asegurar los elementos de prueba, se establecerá una cadena de custodia que resguardará su identidad, estado y conservación. Se identificará a todas las personas que hayan tomado contacto con esos elementos, siendo responsables los funcionarios públicos y particulares intervinientes".

Sin embargo, tal como lo afirma Blanco (2020),

> [...] de la norma no surge cuál es la consecuencia procesal del incumplimiento de la cadena de custodia dirigida a 'asegurar los elementos de prueba'. La doctrina y la jurisprudencia están divididas al respecto: por un lado, un sector entiende que la utilización correcta de la cadena de custodia y el cumplimiento de su procedimiento es una garantía vinculada con el derecho de defensa, de modo tal que el respeto de la misma en orden a la recolección y resguardo de la evidencia —de forma tal que permita conocer con exactitud la identidad del material secuestrado con el presentado en el juicio— constituye una forma esencial de observancia imprescindible, cuya vulneración impone la nulidad de lo actuado […] (pp. 745–746).

En la mayoría de los casos jurisprudenciales, ante las eventuales dudas sobre la cadena de custodia, han llevado a restarle valor a la prueba, pero no su exclusión o su admisibilidad (ejemplo de ello es el caso HSBC, iniciado a partir de la filtración de la denominada "Lista Falciani"[15]), sin tomar dimensión de la importancia ni saber diferenciar entre la etapa de recolección y análisis. En el mismo sentido, tampoco se tiene en cuenta que los procedimientos que se exigen en los protocolos son, justamente, para proteger la integridad o autenticidad de la evidencia digital.

Uno de los casos más resonantes de una nulidad por violación a la cadena de custodia es el caso "Jaime"[16] (exfuncionario), quien se encontraba siendo investigado por el delito de enriquecimiento ilícito. En el marco de ese proceso, se ordenó el peritaje sobre las computadoras secuestradas en el domicilio de la persona.

[15] Juzgado Penal Económico N° 11, HSBC Bank Argentina SA y Otros s/ ley 25.769, causa N° 1652/2014.

[16] Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, Sala I, "Fiscal s/ apela declaración de nulidad de informe pericial", causa N° 46744, resuelto el 24/05/2012. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/5275.

La defensa planteó la nulidad porque no habían sido notificados de la pericia informática de las computadoras secuestradas bajo el argumento de que se trataba de una operación sencilla y reproducible en el futuro. Y que, si bien fueron notificados de una nueva pericia, advertían, a partir del peritaje realizado por los expertos de la UBA, que el material recibido no había sido debidamente resguardado y que la cadena de custodia se encontraba comprometida.

Por tanto, solicitaron que se anularan ambos peritajes, el primero por la omisión de practicar la notificación como establece la normativa procesal, y el segundo por la sospechosa contaminación de la evidencia que fuera advertida por los peritos de la UBA.

La Cámara Federal en lo Criminal y Correccional, valoró los dictámenes de los peritos, entre lo que se destacó que no se registraron adecuadamente las fechas y horas de obtención inicial ni las intervenciones periciales posteriores, como así también que faltaban detalles sobre los métodos utilizados para evitar la contaminación de la evidencia.

Asimismo, expresaron que, a diferencia de los peritos de la UBA, que utilizaron bloqueadores de escritura para proteger los discos duros, los peritos policiales no implementaron mecanismos técnicos para preservar la integridad de los datos. Por otro lado, se hallaron archivos con fechas de modificación anteriores a las de creación, lo que constituye una anomalía técnica inexplicable, según los informes periciales.

Otro precedente en donde declararon la nulidad es el de la Sala IV de la Cámara en lo Criminal y Correccional "F.J.G. s/ Nulidad"[17], en el que se mencionan algunos aspectos que deben tenerse en cuenta al momento de secuestrar o manipular evidencia digital que va a incorporarse al proceso. Entre los principales argumentos, se destaca que ninguna acción del personal policial debe modificar los datos almacenados en computadoras o dispositivos, ya que estos pueden constituir evidencia judicial.

Asimismo, la Cámara afirmó que la evidencia digital es especialmente vulnerable a modificaciones, incluso de forma involuntaria, lo que requiere un manejo más cuidadoso y especializado. Sólo una persona competente y capacitada puede hacerlo, debiendo explicar la relevancia de sus actos y sus posibles consecuencias sobre la integridad de la prueba.

Como conclusión parcial, se puede afirmar que es importante que en la fase de recolección se respeten los protocolos y guías de buenas prácticas, como así también —a fin de garantizar el derecho de defensa de la persona imputada— es fundamental notificar a la defensa para que pueda controlar la primera extracción del contenido, ya que en el dispositivo no sólo se puede hallar prueba de cargo sino también puede existir prueba que sea favorable para la estrategia de defensa. Si no se adoptan medidas diligentes al momento de manipular los dispositivos y la evidencia digital, esta se puede perder o poner en duda su eficacia probatoria.

5. LOS DATOS DE GEOLOCALIZACIÓN COMO EVIDENCIA

[17] Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala VI, "FJG", CCC 37443/2018/2/CA2, resuelto el 31/07/2018. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/1921.

Las herramientas forenses permiten –dependiendo del caso– extraer el contenido del dispositivo y, entre esa información, se puede obtener los datos de ubicación.

Algunos de los datos de ubicación que pueden recuperarse y analizarse son: datos de GPS que registran las coordenadas casi exactas de la ubicación del dispositivo en un momento dado, información sobre las redes wifi a las que se ha conectado el dispositivo, datos de aplicaciones específicas que utilizan la ubicación del dispositivo (por ejemplo, de redes sociales como Instagram o de deportes como *Nike Run Club*), fotografías o videos que se encuentran geolocalizados —con fecha y hora—, etcétera (KeepCoding, 2024).

Si los servicios de ubicación de una aplicación están activados, se pueden recopilar datos de geolocalización incluso cuando la aplicación no está en uso. Además, los dispositivos móviles con cobertura celular escanean constantemente el área en busca de la estación de telefonía más cercana y envían un *ping* a la ubicación del dispositivo cada cierta cantidad de minutos, independientemente de si el dispositivo o alguna aplicación están en uso. Esto genera una CSLI (*Cell Site Location Information*), que generalmente queda almacenada por el proveedor de servicios celulares (Ettari, 2021).

¿Para qué sirve esto a la acusación o a la defensa? Uno de los aspectos más valiosos de los datos de geolocalización es que pueden servir para reconstruir una secuencia de eventos que condujeron antes, durante y después de un hecho delictivo. Esta cronología detallada puede ser vital para comprender la dinámica del hecho.

También las personas involucradas en un hecho suelen proporcionar coartadas que pueden verificarse o refutar mediante datos de geolocalización. Si una persona afirma haber estado en un lugar diferente al momento del delito, los datos de geolocalización pueden confirmar o refutar esa declaración.

Los datos de geolocalización no solamente se generan a través del teléfono celular, sino también a través de dispositivos que llevamos junto a nosotros. Existen varios casos judiciales en diferentes países en los que los datos de relojes inteligentes (smartwatches), como los de *Fitbit*, *Apple Watch*, etc., han sido relevantes al momento de una investigación criminal. En Inglaterra un jurado encontró culpable a Mark Fellow, alias "*Iceman*", de homicidio. Como parte de una de las pruebas que lo incriminaba, se utilizó los datos del GPS de su reloj Garmin, para establecer la ruta y que, concretamente, había pasado —y disminuido la velocidad— al acercarse al vecindario de la víctima (Planeta Triatlón, S.f.)

Sin embargo, se debe tener cuidado debido a la posibilidad de interpretaciones incorrectas y la susceptibilidad a la manipulación. La configuración del dispositivo y las acciones del usuario pueden afectar la precisión de los datos de geolocalización, lo que puede provocar errores en el análisis forense.

Ejemplo de ello son los metadatos que contienen las imágenes y/o videos: pueden contener información sobre la fecha, la hora, el dispositivo que sacó la foto/video y la geolocalización, pero si no se tiene conocimientos técnicos, puede pasar inadvertido que estos datos han sido manipulados. Esto se puede lograr no solo al cambiar la configuración del teléfono, sino que además existen diversas herramientas que permiten

a los usuarios alterar los metadatos de fotos y otros archivos, lo que compromete la integridad de estos datos.

Es crucial corroborar los datos que se obtengan con otras pruebas. Los analistas forenses deben adoptar un enfoque integral, integrando múltiples fuentes de datos, como comunicaciones digitales, declaraciones de testigos y evidencia física, para obtener un panorama más preciso y confiable. Esta estrategia multifacética ayuda a mitigar el riesgo de errores y garantiza un proceso de investigación más exhaustivo y justo.

Es importante saber que no todos los datos de geolocalización son iguales, si no se tiene cuidado al examinarlos, se podrían hacer suposiciones incorrectas sobre la ubicación del dispositivo (Magnet Forensics, 2024).

Establecidas las cuestiones teórico-normativas que regulan la evidencia digital y la geolocalización, a continuación, se analizará un caso paradigmático que ilustra la aplicación práctica de estos conceptos desde la perspectiva de la defensa.

6. ANÁLISIS DE UN CASO

Recientemente, en el caso "L.M.A."[18], hemos podido conseguir la desvinculación del imputado —que se encontraba acusado por el delito de trata con fines de explotación laboral— a través de los datos de geolocalización. En este caso, los datos de geolocalización fueron obtenidos de la pericia informática del dispositivo del denunciante.

Para poner en contexto el hecho, tres personas habían denunciado que se encontraron privados de su libertad durante una semana en el campo en el que cumplían tareas laborales. Se inició la investigación correspondiente por presunto delito de trata de personas y en el marco del proceso uno de los denunciantes se presentó como parte querellante. A fin de acreditar el intercambio de mensajes con el imputado, el querellante procedió a hacer entrega de su dispositivo celular para que se realice la respectiva extracción forense de dichas conversaciones.

Es así como, al notificar el resultado de la pericia del celular del querellante, la defensa analizó el contenido a través de la herramienta UFED READER y en la solapa "ubicaciones del dispositivo" había distintas geolocalizaciones con sus respectivas fechas. A través de su análisis se observó que en las fechas en las que el querellante manifestó presuntamente encontrarse encerrado en el campo, en realidad, estaba ubicado en otros lugares de la ciudad.

A modo de ejemplo, las fotografías del dispositivo mostraban al querellante en la habitación de un lugar —presuntamente un Hospital— junto a un bebé. Es así como, al momento de analizar los metadatos de la fotografía —los cuales surgían en el UFED READER—, la geolocalización era en el Hospital de la ciudad de Concordia. Como consecuencia de ello, dentro de las medidas de pruebas solicitadas, el Juzgado libró oficio

[18] Juzgado Federal de Primera Instancia de Concordia, "L.M.A. s/Infracción artículo 145 bis, conforme Ley 26.842", causa N° 9424/2023, resuelto el 5/11/2024. Disponible en: https://repositorio.mpd.gov.ar/jspui/handle/123456789/5581.

al Hospital para verificar si el querellante había concurrido a dicho nosocomio en esa fecha, lo que arrojó resultado positivo.

Con todas esas medidas probatorias concluidas, en fecha 13 de marzo de 2024, la defensa planteó el sobreseimiento. Para ello, se hizo referencia al resultado de la extracción del contenido del teléfono celular —concretamente de los datos de geolocalización de las fotografías—, y se utilizaron capturas de pantalla de la herramienta UFED READER para que sea visualmente ilustrativo. Así, en el pedido de sobreseimiento se explicó que mientras el denunciante —constituido como querellante— afirmó haber estado encerrado en el campo durante una semana, se había podido demostrar que en esas fechas se encontró geolocalizado en otros lugares.

Es de vital importancia que se comprenda cómo funciona esta herramienta para así poder diagramar estrategias y, en caso de duda, siempre es conveniente realizar la consulta técnica informática respectiva para que, en su caso, mediante un informe técnico especializado en la materia se avale nuestra postura —en caso de que corresponda—.

Finalmente, en fecha 5 de noviembre de 2024 el Juzgado Federal de Concordia dictó su sobreseimiento bajo los siguientes fundamentos:

> [F]ueron citadas y agregadas múltiples fotografías extraídas del peritaje efectuado que la defensa, de acuerdo a sus fechas y geo-localizaciones valoró como prueba sustancial para dar cuenta de que las tres presuntas víctimas se encontraron en múltiples oportunidades fuera del campo, que los horarios que refirieron respecto de la jornada laboral no eran ciertos, y que no emerge ningún tiempo de mensajes donde L. les realice reproches, descuentos de dinero o prohibiciones de ningún tipo. En efecto, la defensa mencionó que ACG manejaba sus horarios, visitaba a su familia, dormía y se higienizaba en su hogar, al igual que su hermano y su tío, a quienes nadie les impedía salir de su lugar de trabajo, trasladarse libremente o dejar de prestar funciones si consideraban que existía un incumplimiento laboral o dinerario.
>
> […] Paralelamente, de las fotografías extraídas del peritaje efectuado y las geo-localizaciones obtenidas se observa, en forma constante, que las tres presuntas víctimas se encontraron en múltiples oportunidades fuera del campo —incluso en el período constatado como constitutivo de la relación laboral—, que los horarios que refirieron respecto de la jornada laboral no resultaron ser ciertos, y que no existen elementos que acrediten que L. les realice reproches, descuentos de dinero o prohibiciones de ningún tipo, por lo que también se encuentra descartado todo tipo de coacción, amenazas o intimidaciones, requeridos por el tipo penal.

Contra esta resolución, la querella presentó un recurso de apelación, el cual fue confirmado por la Cámara Federal de Apelaciones de Paraná, en donde se expresó que:

> […] Se encuentra probado que ACG manejaba sus horarios, visitaba a su familia, dormía y se higienizaba en su hogar, al igual que su hermano y su tío, a quienes de acuerdo a las conversaciones y geo-localizaciones nadie les impedía salir de su

> lugar de trabajo, trasladarse libremente o dejar de prestar funciones si consideraban que existía un incumplimiento laboral o dinerario"[19].

Como se puede observar, la pericia informática resulta de vital importancia para obtener información de geolocalización que puede ser útil para incriminar o desvincular a una persona. Si bien es cierto que no todos los dispositivos almacenan la misma información y dependerá de cada caso en concreto, resulta importante contar con ayuda especializada en la temática a fin de poder realizar un examen técnico exhaustivo del dispositivo para de esta manera no hacer un análisis incorrecto de los hechos o de la prueba.

7. CONCLUSIÓN

La evidencia digital posee características particulares que la hacen frágil, volátil y altamente susceptible a alteraciones, incluso de forma involuntaria. Por este motivo, resulta indispensable respetar rigurosamente protocolos técnicos y legales en todas las fases de su tratamiento: identificación, recolección, preservación, análisis y presentación.

A lo largo del trabajo se detalló la importancia de la cadena de custodia, cuya correcta implementación garantiza la autenticidad e integridad del material probatorio. Su incumplimiento puede derivar en restarle valor probatorio o incluso en la nulidad absoluta de la prueba, como lo han demostrado los precedentes jurisprudenciales mencionados.

También se resaltó la importancia de que la defensa tenga control desde la primera extracción forense y que quienes lleven adelante dicha tarea cuenten con conocimientos técnicos en la materia (*expertise*) para prevenir errores que afecten la evidencia digital.

Entre los datos que se pueden obtener de un dispositivo, los datos de geolocalización han transformado innegablemente el panorama de las investigaciones judiciales, ofreciendo a los investigadores capacidades sin precedentes para localizar con notable precisión donde se ha encontrado un dispositivo y luego utilizarlo como prueba indiciaria en contra de una persona.

En el mismo sentido, y tal como se analizó en el caso llevado adelante por el MPD, esos datos también pueden servir para comprobar nuestra hipótesis defensiva o contrarrestar la acusatoria. Se deben verificar meticulosamente los datos de geolocalización y corroborarlos con otras pruebas y, en su caso, requerir la ayuda técnica especializada de un perito informático de parte de la defensa para garantizar la fiabilidad de la prueba y minimizar errores.

El caso analizado demuestra que los datos de geolocalización extraídos del dispositivo del denunciante permitieron refutar las afirmaciones sobre la privación de la libertad de los denunciantes. Esto evidencia la importancia de realizar un análisis autónomo e independiente de las conclusiones a las que haya arribado el perito informático dependiente del Ministerio Público Fiscal o del Poder Judicial de la Nación.

[19] Cámara Federal de Paraná, "Legajo de apelación de Leonardelli, Mauricio Abraham en autos Leonardelli, Mauricio Abraham por infracción art. 145 bis – conforme Ley 26.842", FPA 9424/2023/4/CA1, resulta el 19/12/2024.

BIBLIOGRAFÍA

Asociación por los Derechos Civiles. (2021). ¿Quién revisa tu teléfono? Primeras aproximaciones a las herramientas de extracción forense de dispositivos móviles en Argentina. https://adc.org.ar/wp-content/uploads/2022/01/ADC-Quien-revisa-tu-telefono.pdf.

Bentin, A. (2024). La pericia informática en el proceso penal: una perspectiva desde la defensa. En M. Riquert & C. C. Sueiro (Eds.), *Sistema penal e informática* (Vol. 7, pp. 122-126). Hammurabi.

Blanco, H. (2020). Tecnología informática e investigación criminal. La Ley.

Center for Democracy and Technology. (2011). *'Going dark' versus a 'golden age for surveillance'*. https://cdt.org/insights/going-dark-versus-a-golden-age-for- surveillance/.

Ettari, S. V. (2021). Using geolocation data in litigation. HSF Kramer. https://www.hsfkramer.com/kl-pdfs/6/2/62740.pdf.

ISO/IEC. (2012). ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Organización Internacional de Normalización.

KeepCoding. (2024). Análisis forense ubicaciones en dispositivo iOS. https://keepcoding.io/blog/analisis-forense-ubicaciones-en-dispositivo-ios/.

Magnet Forensics. (2024). Not all geolocation data is created equal. https://www.magnetforensics.com/blog/not-all-geolocation-data-is-created-equal/.

Ministerio Público de la Defensa & ODIA. (2023). Evidencia digital y derechos humanos: Desafíos jurídicos en la era tecnológica [Boletín]. https://repositorio.mpd.gov.ar/jspui/handle/123456789/5342.

Planeta Triatlón. (s.f.). GPS delata a corredor sicario en la escena del crimen. https://planetatriatlon.com/gps-delata-corredor-sicario-la-escena-del-crimen/.

Reale, J. M. (2023). Importancia de la cadena de custodia en materia de evidencia digital y su tratamiento por la jurisprudencia argentina. En Polansky, J. y Salt, M. (Dir.), *La investigación penal en el entorno digital* (1ª ed.). Hammurabi.

Sueiro, C. C. (2019). *Vigilancia electrónica y otros modernos medios de prueba* (2ª ed.). Hammurabi.

Universidad FASTA & Universidad Champagnat. (2022). Guía de recomendaciones para la implementación de protocolos de actuación para la adquisición, preservación y presentación de la prueba digital – PAFE– CCyLF. Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense.