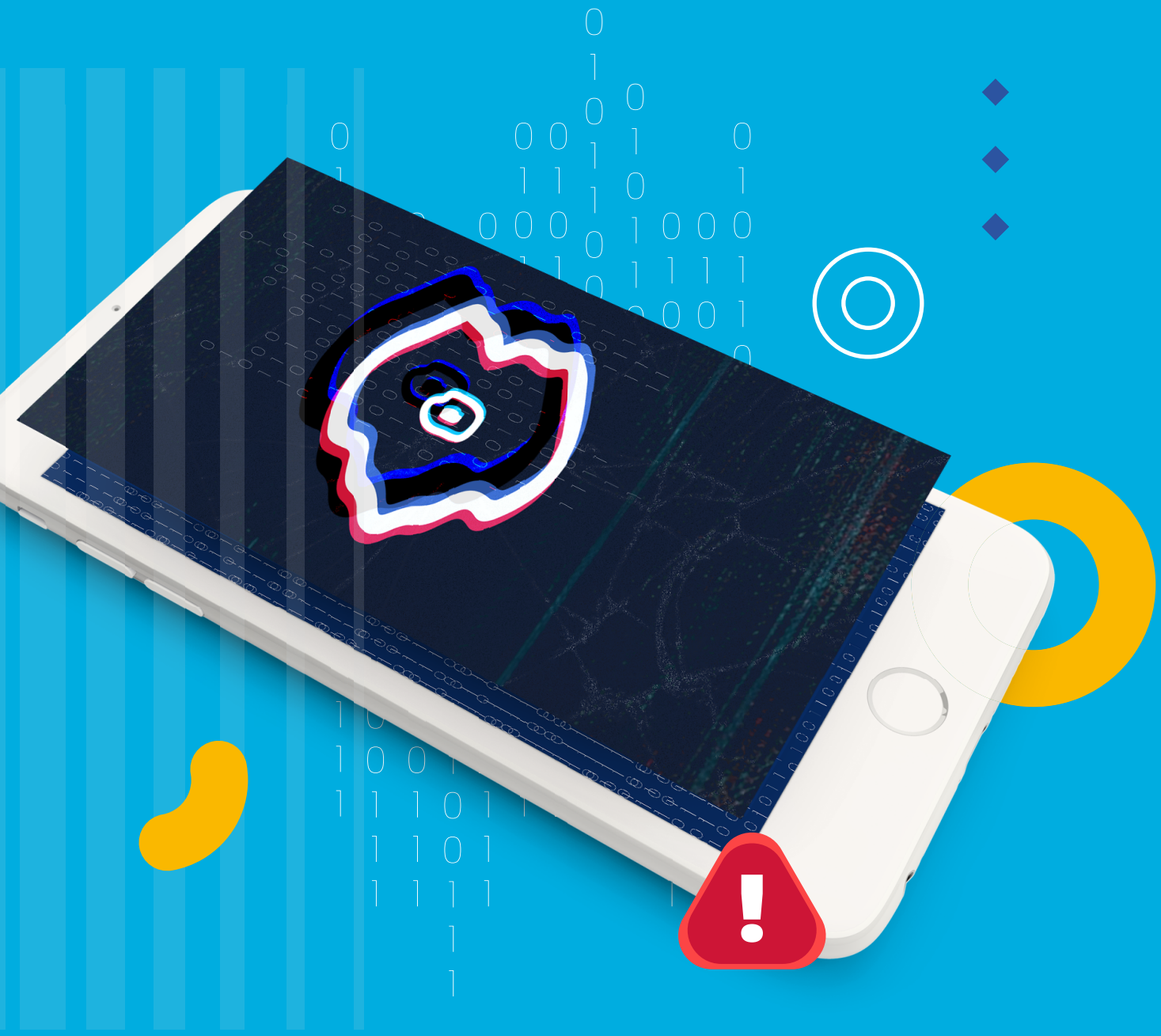
por los Derechos Civiles



¿Quién revisa tu teléfono?

Primeras aproximaciones a las herramientas de extracción forense de dispositivos móviles en Argentina

Diciembre 2021
adc.org.ar

Redacción: Alejo Kiguel
Diagramación y diseño: El Maizal - Cooperativa de Comunicación

Contenido

Resumen Ejecutivo

Fotos, videos, agendas, contactos, detalle de lugares visitados, registro de llamadas entrantes y salientes, mensajes enviados y recibidos, mensajes borrados, resúmenes bancarios, correos electrónicos, notas personales y aplicaciones de todos los tipos son solo parte de la información que se puede encontrar en un celular.

En algunos casos estos datos pueden servir para encontrar al culpable de un delito, determinar si un/a imputado/a estuvo en un lugar específico o conocer las conversaciones que tuvo previo a un hecho delictivo. Más problemático aún, la información que está en nuestro teléfono no solo incluye una enorme cantidad de nuestra información privada, sino también de terceros, como amigos/as, familia o compañeros/as de trabajo. Así, el teléfono celular se ha transformado en el espacio más íntimo que una persona puede tener y al mismo tiempo un valioso elemento probatorio para las investigaciones judiciales.

Ante la necesidad de acceder a la información alojada en dispositivos móviles, y las dificultades técnicas que se presentan, desde hace ya algún tiempo viene creciendo una industria que desarrolla y vende herramientas que tienen como objetivo ofrecer a peritos y auxiliares de la justicia herramientas que permitan acceder y analizar de forma eficiente la información de los teléfonos móviles.

En este informe realizamos un primer acercamiento a cuáles son las herramientas que están siendo utilizadas en Argentina para extraer información de los celulares y quiénes son las empresas que proveen estas tecnologías. Para ello, en un primer momento explicaremos qué son las herramientas de extracción forense de dispositivos móviles, luego quiénes son los/las peritos y auxiliares de justicia que las utilizan y quiénes son los principales proveedores. Por último expondremos algunos de los desafíos que presenta el secuestro y análisis de la

evidencia digital de dispositivos móviles y algunas consideraciones que debieran ser tenidas en cuenta para una regulación que sea respetuosa de los derechos de las personas.

Introducción

El tratamiento y la regulación de la evidencia digital es uno de los mayores desafíos para el derecho penal y procesal penal en la actualidad. Entendida como cualquier "elemento probatorio que surge de medios informáticos, digitales o tecnológicos"[1], la evidencia digital se ha transformado en un elemento fundamental para resolver cualquier investigación. A esta altura no debería llamar la atención que la información que puede encontrarse en una computadora o un teléfono móvil pueda ser relevante para el juzgamiento de cualquier delito, haya sido este cometido a través de medios informáticos o no.

En documentos anteriores analizamos los desafíos que la evidencia digital presenta para las investigaciones penales[2]. Para lo que aquí interesa, basta decir que la regulación clásica de la prueba física no se ajusta de forma adecuada al entorno digital. Las características propias de la evidencia digital –volatilidad, fragilidad, necesidad de conocimientos técnicos para su acceso, entre otros[3]– generan desafíos que en algunos casos requieren la necesidad de sancionar reglas específicas que regulen su tratamiento.

Asimismo, al diseñar reglas específicas se presenta el desafío de respeto de las garantías constitucionales y ser lo suficientemente preciso como para no violar el principio de legalidad[4], pero al mismo tiempo que la norma no quede obsoleta ante cualquier innovación tecnológica.

La obtención y análisis de la evidencia digital muchas veces requiere de conocimientos técnicos específicos. Así, la informática forense se presenta como la disciplina encargada de "aplicar técnicas informáticas en el proceso de adquirir, preservar, obtener y presentar datos que han sido procesados y/o almacenados de forma electrónica y que son relevantes en el ámbito judicial" y tienen un rol cada vez más importante en los procesos judiciales[5]. Los procedimientos que los peritos informáticos realizan en los laboratorios forenses para obtener la

evidencia digital y las herramientas que utilizan resultan fundamentales para determinar la admisibilidad de la prueba en el proceso.

En este contexto, dentro del universo de la evidencia digital, hay un subtipo de evidencia que en el último tiempo ha cobrado especial relevancia y es aquella que surge de los dispositivos móviles, o más específicamente de los teléfonos móviles inteligentes.

En el 2021 en Argentina, 34,8 millones de argentinos y argentinas son usuarios de algún tipo de teléfono móvil inteligente[6]. Fotos, videos, agendas, contactos, detalle de lugares visitados, registro de llamadas entrantes y salientes, mensajes enviados y recibidos, mensajes borrados, resúmenes bancarios, correos electrónicos, notas personales y aplicaciones de todos los tipos son solo parte de la información que se puede encontrar en un celular.

En algunos casos esta información puede servir para encontrar al culpable de un delito, determinar si un/a imputado/a estuvo en un lugar específico o conocer las conversaciones que tuvo previo a un hecho delictivo. Más problemático aún, la información que está en nuestro teléfono no solo incluye una enorme cantidad de información privada nuestra, sino también de terceros como amigos/as, familia, compañeros/as de trabajo, etc. Así, el teléfono celular se ha transformado en el espacio más íntimo que una persona puede tener y al mismo tiempo un valioso elemento probatorio para las investigaciones judiciales.

Ante la necesidad de acceder a la información alojada en dispositivos móviles, y las dificultades técnicas que se presentan, desde hace ya algún tiempo viene creciendo una industria que desarrolla y vende herramientas que tienen como objetivo brindar a los/las peritos y auxiliares de la justicia de herramientas que permitan acceder y analizar de forma eficiente la información de los teléfonos móviles.

En este informe realizamos un primer acercamiento a cuáles son las herramientas que están siendo utilizadas en Argentina para extraer información de los celulares y quiénes son las empresas que proveen estas tecnologías. Para ello en un primer momento explicaremos qué son las herramientas de extracción forense de dispositivos móviles, luego quiénes son los/las peritos y auxiliares de justicia que las utilizan y quiénes son los principales proveedores. Por último presentaremos algunos de los desafíos que presenta el secuestro y análisis de la evidencia digital de dispositivos móviles y algunas consideraciones que debieran ser tenidas en cuenta para una regulación que sea respetuosa de los derechos de las personas.

¿Qué son las herramientas de extracción forense de dispositivos móviles y quién las utiliza?

Cuando hablamos de herramientas de extracción forense de dispositivos móviles nos referimos a herramientas diseñadas para extraer toda la información posible de un dispositivo móvil a través de técnicas informáticas forenses que permitan incorporar de forma adecuada la información obtenida a un proceso judicial.

En el contexto de las investigaciones penales, estas prácticas son llevadas a cabo por peritos informáticos o en laboratorios informáticos que dependen de fuerzas de seguridad y de la ley nacionales y provinciales[7]. Actualmente tanto las fuerzas y fiscalías federales como la mayoría de las fiscalías provinciales cuentan con herramientas para llevar adelante estas prácticas.

Entre las dependencias que fueron analizadas para este informe se encuentran: Gendarmería Nacional Argentina (GNA), Policía Federal Argentina (PFA), Policía de Seguridad Aeroportuaria (PSA), Ministerio Público de la Ciudad Autónoma de Buenos Aires, Policía de la Ciudad Autónoma de Buenos Aires, Ministerio Público de Salta, Ministerio Público Fiscal de Santiago del Estero, Gabinete Científico del Poder Judicial de Chacho, Ministerio Público de Chubut, Ministerio Público de la Provincia de Buenos Aires, Ministerio Público de Córdoba, Ministerio Público de Jujuy y Ministerio Público de Santa Fe.

Herramientas y proveedores

Las fuerzas de seguridad y de la ley utilizan diversas herramientas de extracción forense de dispositivos móviles fabricadas por empresas privadas. En este capítulo nos concentraremos en los proveedores que mayor presencia tienen a nivel mundial y sobre las que se pudo obtener información de que estarían siendo utilizadas en Argentina.

UFED de Cellebrite

Cellebrite es una compañía isrealí subsidiaria de la empresa japonesa Suncorporation ltd fundada en 1999 como una empresa de inteligencia artificial. Entre sus servicios, Cellebrite ofrece "la gama más completa y probada de la industria de soluciones de ciencia forense digital, triage y estudio analítico"[8] a cuerpos de seguridad, militares y de inteligencia y clientes empresariales de todo el mundo[9].

En el 2007 lanzó por primera vez el "Universal Forensic Extraction Device" (UFED), que hoy se ha convertido en una de las principales herramientas utilizadas por fuerzas de seguridad, inteligencia, y agentes de la ley en el mundo para extraer información de dispositivos móviles[10].

Las herramientas de Cellebrite permiten acceder a una amplia variedad de dispositivos entre los que se encuentran los teléfonos con sistema operativo Android e IOS, drones, tarjetas SIM y SD y dispositivos GPS, entre otros. Desde su lanzamiento, la compañía ha actualizado múltiples veces su herramienta, siendo que al día de hoy ofrece al menos 10 productos asociados[11].

La herramienta principal de Cellebrite es el UFED que permite "realizar extracciones lógicas, físicas y de sistema de archivo, acceder a dispositivos bloqueados y funciona con más de 31 mil modelos de dispositivos móviles"[12]. La herramienta se vende como un software

para ser instalado en cualquier PC (UFED 4PC) o en su versión UFED Touch2, que incluye una tablet portátil y accesorios que permiten realizar la extracción en cualquier lugar.

Además de las herramientas de extracción propiamente dichas, Cellebrite también vende una línea de productos destinados al análisis de la información obtenida (Cellebrite Pathfinder y Cellebrite Inspector) que en algunos casos permiten realizar búsquedas automatizadas de personas, lugares u objetos en imágenes[13].

En Argentina, a pesar de tratarse de herramientas de alto costo[14], también se ha posicionado como la herramienta más utilizada para extraer y analizar información en dispositivos móviles[15]. Según fuentes periodísticas, la cantidad de licencias que actualmente se encontrarían activas en Argentina ascendería a 350[16].

Del relevamiento que pudimos realizar, el cual incluyó pedidos de acceso a la información pública, entrevistas y relevamientos en Internet, pudimos relevar que la tecnología de UFED estaría siendo utilizada al menos por los siguientes cuerpos de investigación:

Gendarmería Nacional Argentina[17]:

En total cuenta con 18 laboratorios digitales en todo el país y al menos 35 licencias de la herramienta UFED[18], constituyéndose así como uno de los principales compradores y usuarios de la tecnología de Cellebrite en el país. En su página oficial, Cellebrite presenta los laboratorios de Gendarmería como un caso de éxito de sus herramientas[19].

En septiembre del 2019, la GNA adquirió una estación de trabajo para desbloquear teléfonos inteligentes de alta gama[20] a través de un contrato directo con Security Team Network S.A. por un total de 643.900 dólares[21]. En noviembre del mismo año, la Dirección de

Criminalística y Estudios Forenses de Gendarmería adquirió cuatro licencias para el software "UFED 4PC". La adquisición se realizó a través de una licitación pública en la que la empresa Security Team Network resultó adjudicataria por un monto total de 9.587.400 pesos (alrededor de 159.000 dólares en ese momento)[22]. Más recientemente, Gendarmería actualizó esas licencias en junio del 2020, en un contrato con Security Team Network por un total de 132.116 dólares[23].

Policía de Seguridad Aeroportuaria (PSA):

En diciembre del 2020 celebró un contrato directo con IAFIS Argentina S.A. para actualizar y mejorar sus licencias de UFED por un total de 8.057.111 pesos (aproximadamente 90.784 dólares). El contrato incluía la renovación de dos licencias UFED 4PC Ultimate y dos de UFED Touch 2 Ultimate[24] por una duración de dos años y también la permuta de hardware de dos dispositivos Touch I por dos UFED Touch 2[25].

Policía Federal Argentina:

A través de las divisiones de Apoyo Tecnológico Judicial, Delitos Tecnológicos e Informática Forense, también utilizaría la herramienta UFED para extraer información de dispositivos móviles. Aunque no se pudieron encontrar documentos que den cuenta sobre cómo fueron los procesos de compra de estas herramientas, su utilización en distintas causas judiciales[26] permite inferir que la PFA contaría al menos con 3 licencias de UFED[27] [28].

Prefectura Naval Argentina:

También utiliza la herramienta UFED. En el 2020 se distribuyeron nuevas licencias en distintas dependencias de la Sección Científico Pericial[29].

A nivel provincial, la utilización de UFED también se encuentra ampliamente consolidada en los Ministerios Público Fiscales y fuerzas de seguridad. A modo de ejemplo:

Laboratorios Regionales de Investigación Forense:

En 2010 el Ministerio de Justicia y Derechos Humanos de la Nación impulsó el desarrollo de laboratorios forenses en todo el país. Así, a través de convenios con distintas jurisdicciones, brindó recursos económicos y herramientas para equipar los laboratorios. Un documento oficial del Ministerio de Justicia informó que entre el equipamiento distribuido se encontraba la herramienta UFED de Cellebrite[30]. En octubre de 2021, en una nueva addenda al convenio, se acordó que el Ministerio de Justicia y Derechos Humanos de la Nación destinará 125.000.000 pesos para la creación e implementación de Laboratorios Regionales de Investigación Forense, donde parte de los fondos estarán destinados a actualizar las licencias de UFED adquiridas por los ministerios públicos de distintas provincias[31]. Entre los laboratorios que se vieron beneficiados por dicha iniciativa se encuentran los de Entre Ríos[32], Mendoza, San Juan, San Luis, Formosa, Neuquén, Chubut, La Pampa, Corrientes; y Misiones[33].

Otros ejemplos de su utilización son:

Ministerio Público Fiscal de Salta:

Cuenta con la tecnología de UFED4PC y UFED TOUCH al menos desde 2018, cuando renovó sus licencias mediante un contrato directo con Security Team Network[34].

En 2019, la provincia también habría adquirido el producto Cellebrite UFED Infield a través de una "adquisición realizada con aportes crediticios del estado provincial"[35]. Adicionalmente, en 2021, Salta formó parte del acuerdo para recibir fondos del Ministerio de Justicia de la Nación para renovar sus licencias de UFED[36]. En septiembre de ese año renovó[37] una licencia de software UFED ULTIMATE TOUCH2 y una licencia de software UFED CLOUD a través de una licitación con la firma VEC SRL por la suma de 1.430.370 pesos[38].

Gabinete Científico del Poder Judicial de Chaco (GCJ):

En la provincia al menos desde 2014 cuentan con la herramienta UFED para realizar extracciones forenses de dispositivos móviles. Las herramientas se encuentran bajo la órbita del GCJ[39], que sería el único que cuenta con esta tecnología en la provincia[40]. La adquisición de estas herramientas se realizó a través del Ministerio de Justicia y Derechos Humanos de la Nación y la iniciativa de impulsar el desarrollo de Laboratorios Regionales de Investigación Forense.

Ministerio Público Fiscal de Santiago del Estero:

La "Memoria Institucional 2017-2018" de esta cartera da cuenta de que el área de Informática Forense del Gabinete de Ciencias Forenses del MPF cuenta con la herramienta UFED Touch2 para la extracción de dispositivos móviles[41].

Ministerio Público Fiscal de Chubut:

A través del Equipo Técnico Multidisciplinario con Sede en Comodoro Rivadavia utiliza la tecnología de UFED Cellebrite para la extracción de datos de equipos móviles[42].

Ministerio Público Fiscal de la Provincia de Buenos Aires:

Según surge de su reporte anual[43], en 2020 se utilizó la tecnología de UFED4PC en más de "10.000 efectos, entre dispositivos móviles, tarjetas de memoria y SIM Card". Entre las dependencias que cuentan con esta herramienta se encuentran la Oficina de Gestión de Información Tecnológica (OFITEC) de Mercedes, el Laboratorio Forense de Comunicaciones Complejas de Mar del Plata, y la Fiscalía General de Bahia Blanca[44], entre otros.

Policía de la Ciudad Autónoma de Buenos Aires:

La Dirección de Delitos Informáticos, la División de Análisis de Inteligencia Informática y la Sección de Investigaciones Especiales utilizan las herramientas UFED4PC, UFED TOUCH2 y UFED AnalyticsPathfinder Desktop para la extracción y análisis de

dispositivos móviles. En 2021 se realizó una licitación pública[45] para renovar por el plazo de 24 meses siete licencias de UFED4PC, dos licencias de UFED TOUCH y una licencia de UFED AnalyticsPathfinder. El monto total de la contratación fue de 29.278.296 pesos.

Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires:

Cuenta con 10 licencias UFED4PC y dos licencias KIOSK INFIELD también de Cellebrite que son renovadas anualmente. En el 2020 el costo de la renovación de licencias fue de 171.087 dólares[46] y en 2021 se renovaron por 119.161 dólares[47]. En ambos casos el adjudicatario de la licitación pública[48] fue la empresa IAFIS S.A., que resulta ser uno de los principales distribuidores de la tecnología de la empresa Cellebrite en Argentina.

Anteriormente, en el 2019 se habían adquirido dos licencias de UFED4PC mediante licitación pública con la empresa Security Team Network por la suma de 27.000 dólares[49]. Estos productos fueron destinados al Cuerpo de Investigaciones Judiciales[50]. Este centro ya había renovado una licencia de otro producto, UFED Cloud Analyzer, en el 2017, también mediante un contrato directo con la misma empresa local[51].

Ministerio Publico Fiscal de Santa Fe:

En agosto del 2020, la Fiscalía General de la provincia firmó un contrato directo con la empresa local IAFIS Argentina S.A. para renovar cuatro licencias de UFED Touch 2 por un plazo de un año y adquirir tres licencias nuevas de UFED 4PC, por un total de 96.226[52] dolares[53].

Ministerio Público Fiscal de Córdoba:

Al menos desde 2013 utiliza la tecnología de UFED Cellebrite. En 2015 se llamó a una licitación pública[54] para adquirir “un (1) conjunto de hardware y software para análisis y extracción de datos forenses de dispositivos móviles, tipo UFED SYSTEM + UFED CLOUD ANALYZER de

CELLEBRITE o calidad superior" con un presupuesto de 828.120 pesos. En 2020 "incorporó a la Unidad de Equipos Móviles del Gabinete de Tecnología Forense de la Dirección de Análisis Criminal y Tecnologías de la información de un equipo UFED 4PC, para extraer información contenida en un dispositivo móvil"[55].

La información hasta aquí mencionada permite dar una idea del alcance que la herramienta UFED de Cellebrite tiene en nuestro país. Fuentes periodísticas informan que en total en Argentina existirían más de 350[56] licencias de UFED, por lo que es de esperar que los casos aquí mencionados sólo muestran un pequeño porcentaje del total de las contrataciones que se efectúan en Argentina para poder contar con esta tecnología.

XRY de MSAB

MSAB es una compañía de origen sueco fundada en 1984 que se especializa en el desarrollo de herramientas de extracción y análisis de dispositivos móviles. Entre sus clientes se encuentran "fuerzas de seguridad, instituciones penitenciarias, agencias de inteligencia, autoridades tributarias, organismos de control de fronteras, ejército y ciertas empresas privadas"[57].

La herramienta principal de MSAB para la extracción forense de dispositivos móviles es la XRY, que a su vez tiene una línea de productos entre los que se encuentran:

- **XRY Logical**[58]**:** Promocionado por la empresa como su producto más vendido, permite realizar una extracción lógica del dispositivo y acceder y recuperar cualquier sistema de archivo del dispositivo en tiempo real.
- **XRY Physical**[59]**:** El segundo modelo de XRY permite realizar una extracción física del dispositivo. Este modelo permite eludir el sistema operativo del dispositivo y así acceder a datos borrados

y en algunos casos vulnerar el cifrado si el dispositivo se encuentra bloqueado.

- **XRY Cloud**[60]**:** XRY Cloud es una herramienta de extracción que permite a los examinadores forenses recuperar datos en la nube. Según promociona la empresa, XRY Cloud permite acceder a información de servicios como Facebook, Google, iCloud, Twitter y Snapchat sin necesidad de introducir los datos de usuario y contraseña.

El principal mercado de XRY se encuentra en Europa y más específicamente en Reino Unido, donde es el proveedor del 97% de las fuerzas de seguridad[61].

En Argentina, se encontraron registros de uso por parte de fuerzas de seguridad y de la ley al menos desde 2014. El precio estimado de un XRY complete kit-Mobile forensic tool que incluye el hardware y software necesarios para realizar una extracción forense es de 7.990 dólares[62] con una licencia anual que luego hay que renovar por otros 3.000 dólares[63].

Algunas de las fuerzas de seguridad y de la ley que tienen esta tecnología son: el Ministerio Público Fiscal de la Nación[64] a través de la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal; el Ministerio Público Fiscal de Río Negro[65]; el Poder Judicial de Chaco a través del Gabinete Científico Judicial[66]; el Ministerio Publico Fiscal de la Provincia de Buenos Aires[67] y Santiago del Estero, donde el Ministerio Público Fiscal provincial tiene esta herramienta al menos desde el 2014[68].

La obtención de la herramienta en este último caso se produjo a través de una donación registrada en la Resolución 51/2014, la cual incluyó la herramienta XRY OFFICE compuesta por el hardware y el software XRY Logical[69]. Aunque no se encontraron registros de nuevas adquisiciones,

la “Memoria Institucional 2017-2018” del Ministerio Público Fiscal de Santiago del Estero da cuenta de que en la actualidad la herramienta se encontraría en el área de Informática Forense del Gabinete de Ciencias Forenses del MPF[70].

Por su parte, la Policía Federal Argentina realizó en el 2018 una licitación nacional para adquirir siete dispositivos para extracción de datos de aparatos de telefonía celular móvil, marca XRY versión complete con licencia por treinta y seis meses[71].

Magnet AXIOM de Magnet Forensics

Magnet Forensic[72] es una empresa de origen canadiense fundada en el 2010 que se dedica a desarrollar software de investigación digital para adquirir, analizar, informar y gestionar pruebas de fuentes digitales. Entre sus clientes se encuentran fuerzas de la ley, de seguridad y empresas.

Su principal producto es el Magnet AXIOM[73], que permite recuperar evidencia digital de diversos equipos informáticos, incluidos los smartphones, servicios en la nube, y computadoras, entre otros[74]. En lo que respecta a dispositivos móviles, AXIOM afirma que puede “encontrar fotos, chats e historial de navegación de dispositivos iOS y Android”. Además, permite recuperar y analizar los datos de muchas aplicaciones cifradas que se encuentren instaladas en el dispositivo.

En Argentina, algunas de las fuerzas de seguridad y de la ley utilizan el software AXIOM. En el 2020 el Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires renovó 6 licencias por un año de Magnet AXIOM con servicio de soporte y actualizaciones para uso del Cuerpo de Investigaciones Judiciales por un monto de 2.379.972 pesos[75].

Anteriormente, en el 2019 se había producido una renovación de las mismas 6 licencias de Magent AXIOM por la suma de 21.000 dólares[76].

La Policía de la Ciudad Autónoma de Buenos Aires, a través de la Dirección de Delitos Informáticos, la División de Análisis de Inteligencia Informática y la Sección de Investigaciones Especiales también utiliza la herramienta AXIOM[77]. En diciembre de 2020 el Ministerio Público Fiscal de Santa Fe adquirió un software Magent Axiom Complete para el análisis forense de computadoras y dispositivos móviles y una licencia de Magnet Axiom Cloud por el monto de 1.330.200 pesos[78]. El Ministerio Público de la Provincia de Jujuy renovó en el 2020 una licencia de Magent AXIOM a través de su departamento de Informática Forense perteneciente al Organismo de Investigaciones de este Ministerio[79].

Hasta aquí se mencionaron algunas de las principales herramientas utilizadas por las fuerzas de seguridad y de la ley en Argentina. A nivel mundial, los dos principales proveedores son Cellebrite con su herramienta UFED y MSAB con la herramienta XRY. En Argentina, la herramienta UFED es la más utilizada para la extracción forense de dispositivos móviles. Otras herramientas que no fueron analizadas en este informe pero que también pueden ser utilizadas para la extracción y análisis de dispositivos móviles son Encase Mobile y Oxygen Forensic, entre otras. Además, existe una industria de desarrolladores de herramientas de código abierto, sobre las cuales se abordarán algunos aspectos en el próximo apartado.

La importancia de los códigos fuente

Del relevamiento realizado hasta ahora, el lector podrá haber advertido 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[80] y suele ser comercializado a título oneroso[81]. Así, una etapa fundamental de los procesos, que constituye nada menos que la obtención de prueba que podrá determinar la culpabilidad o inocencia de una persona, es llevada a cabo mediante herramientas y programas cuyos códigos y algoritmos de funcionamiento se desconocen.

Esto podría presentar un desafío frente al artículo 18 de la Constitución Nacional que reconoce al imputado de un delito la facultad de poder conocer y controlar la prueba que se utiliza en su contra[82]. Cierta doctrina nacional[83] y jurisprudencia extranjera[84] sostiene que una prohibición absoluta de este tipo de programas, por el simple hecho de no conocer en detalle los códigos y algoritmos sobre cómo funcionan, no es razonable. De acuerdo a esta postura, y dado que existirían dificultades en el acceso a herramientas de software libre para desbloquear y extraer datos de dispositivos móviles, una prohibición absoluta dejaría a la justicia sin la posibilidad de contar con un elemento de prueba de relevancia[85].

En este sentido, cabe destacar que el secreto comercial es un interés legítimo y protegido por el derecho. Sin embargo, no puede ser invocado en situaciones que puedan afectar derechos fundamentales como el derecho de defensa mencionado anteriormente. La admisibilidad de estas herramientas en un proceso judicial debe estar condicionada a que garantice a través de cualquier medio que

la herramienta sigue una metodología confiable y que los resultados que se obtienen no han sido alterados. Para ello, promover la transparencia y control sobre cómo funcionan estas herramientas es indispensable para supervisar el funcionamiento de los dispositivos y detectar posibles defectos que podrían afectar la confiabilidad de la prueba producida.

A modo de ejemplo, en abril de 2021 el CEO de la empresa proveedora de servicios de mensajería instantánea Signal denunció que había encontrado vulnerabilidades en la herramienta UFED de Cellebrite[86]. A través de programas instalados en cualquier aplicación de un teléfono, podrían infectar el programa de la herramienta forense de Cellebrite, planteando así dudas sobre la fiabilidad de los resultados que la herramienta ofrece a la justicia.

Según explicó "al incluir un archivo especialmente formateado en una aplicación de un dispositivo que luego es escaneado por Cellebrite, sería posible ejecutar un código que modifique no sólo el informe de Cellebrite que se está creando en ese escaneo, sino también todos los informes de Cellebrite anteriores y futuros generados por todos los dispositivos previamente escaneados y todos los dispositivos futuros escaneados de cualquier manera arbitraria (insertando o eliminando texto, correo electrónico, fotos, contactos, archivos o cualquier otro dato)"[87]. La noticia puso en duda la legitimidad de la herramienta e incluso en tribunales de los Estados Unidos se realizaron planteos judiciales solicitando que se revisen sentencias que habían tenido como único fundamento evidencia aportada por la herramienta de Cellebrite[88].

Como fue mencionado anteriormente, la utilización de herramientas forenses de software comercial deben ser examinadas cuidadosamente para que no se afecte el derecho a la defensa en juicio del artículo 18 de la Constitución Nacional. La detección de fallas o vulnerabilidades en determinadas herramientas, que podrían poner en duda la fiabilidad de la prueba obtenida, debe ser tenida en

cuenta por los operadores judiciales para elegir una herramienta por sobre otra. Además, la falta de conocimiento sobre la metodología aplicada dificulta un adecuado control de los programas utilizados. Aquí, aunque su desarrollo es aún muy incipiente[89], la utilización de programas de software abierto, donde el código fuente es público, podría ser una alternativa que facilite al imputado el control de las herramientas que se están utilizando en su contra.

Consideraciones Finales

El trabajo hasta aquí expuesto pretendió realizar una descripción de las principales herramientas que se están utilizando en Argentina para la extracción de datos de dispositivos móviles.

La sensibilidad de la información que tienen en la actualidad nuestros teléfonos celulares requiere que las prácticas mediante las cuales se llevan adelante las tareas de extracción y análisis de datos, así como la normativa que permite incorporarlas en un proceso judicial sean respetuosas de las garantías del imputado. La apertura y análisis de un dispositivo móvil constituye una de las medidas disponibles más invasivas de la privacidad y, por lo tanto, cuando un juez ordena su extracción y análisis debe hacerlo aplicando estrictos criterios de necesidad y proporcionalidad que justifiquen la medida. Esto requiere en parte repensar el concepto de privacidad, el cual tradicionalmente se encuentra vinculado a la idea de propiedad sobre un espacio cerrado[90]. Para ello se deben diseñar reglas específicas que tengan en cuenta las particularidades que la tecnología presenta y así aumentar las protecciones a los individuos con el fin de garantizar una efectiva protección de derechos.

Además debe tenerse presente que la extracción de dispositivos móviles suele producir información relevante para la investigación, pero también una gran cantidad información personal del usuario que nada tenga que ver con el objeto de la causa. 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[91].

En cuanto a las empresas, debido al rol que tienen en el desarrollo y venta de estas tecnologías, debe procurarse promover la transparencia en las contrataciones y en el desarrollo. Si bien las compañías pueden tener legítimas razones para no brindar datos por cuestiones de propiedad intelectual, esto de ninguna manera debe significar que acusados o imputados carecerán de la información necesaria para planear su defensa. En este sentido, existen mecanismos que permiten un mayor control sobre cómo funcionan para evitar vulneraciones de derechos. A modo de ejemplo, podrían generarse espacios donde las empresas puedan explicar el funcionamiento de los programas o incentivar la innovación de forma tal que los algoritmos sean diseñados para poder ser auditados por terceros independientes[92].

Además, en el desarrollo de las tecnologías las empresas deben comprometerse a respetar los derechos humanos. Para ello, la guía "¿Cómo implementar la debida diligencia en derechos humanos en el desarrollo de tecnología?"[93] desarrollada por ADC incluye consideraciones a tener en cuenta para un desarrollo respetuoso de los derechos humanos. Por ejemplo, cuando las herramientas incluyen programas de reconocimiento facial que en el análisis de imágines permiten identificar personas, debieran tener en cuenta los riesgos de discriminación que estas tecnologías presentan. Lo mismo puede suceder con otras funcionalidades de las herramientas que puedan utilizar inteligencia artificial.

A modo de conclusión, el tratamiento y regulación de la evidencia que surge de los dispositivos móviles resulta fundamental para el derecho penal y procesal penal por su relevancia en todo tipo de investigaciones. Conocer cómo funcionan los procedimientos mediante los cuales las fuerzas de seguridad y de la ley pueden acceder a estos equipos es indispensable para garantizar un diseño normativo respetuoso de los derechos humanos. Para ello, la transparencia en el desarrollo de las tecnologías y en su contratación con el Estado resulta indispensable para que exista un control adecuado.

Notas

1 / ADC, "Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina, Vol. II", 2018, https://adc.org.ar/wp-content/uploads/2019/06/038-analisis-juridico-de-la-situacion-de-la-evidencia-digital-en-el-proceso-penal-en-argentina-vol-3-04-2018.pdf pag.2

2 / Ibid

3 / Para un mayor detalle sobre las caracteristicas propias de la evidencia digital, ver el informe publicado por ADC en 2018, "Analisis juridico de la situación de la evidencia digital en el proceso penal en Argentina", disponible en https://adc.org.ar/wp-content/uploads/2019/06/038-analisis-juridico-de-la-situacion-de-la-evidencia-digital-en-el-proceso-penal-en-argentina-vol-3-04-2018.pdf

4 / Artículo 18 de la Constitución Nacional.

5 / Informática forense: el camino de la Evidencia digital, Mariano EnriqueTorres, disponible en http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/informatica_forence.htm

6 / Número de usuarios de teléfonos móviles inteligentes en Argentina de 2015 a 2025 https://es.statista.com/estadisticas/598527/numero-de-usuarios-de-moviles-en-argentina/

7 / ADC, "La investigación forense informática en America Latina", 2018, https://adc.org.ar/wp-content/uploads/2019/06/037-la-investigacion-forense-informatica-en-america-latina-vol-2-04-2018.pdf

8 / Página oficial de Cellebrite, https://www.cellebrite.com/es

9 / Según fuentes periodísticas, Cellebrite tiene el 65% del mercado mundial de herramientas de extracción forense de dispositivos móviles. https://www.clarin.com/policiales/detectives-telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html

10 / Ibid

11 / Detalle de productos y actualizaciones **https://www.cellebrite.com/es/actualizaciones-de-los-productos/**

12 / Web oficial de Cellebrite **https://cf-media.cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf**

13 / Web oficial de Cellebrite **https://cf-media.cellebrite.com/wp-content/uploads/2020/08/ProductOverview_Cellebrite_Pathfinder.pdf**

14 / El costo de un toolkit UFED sería de aproximadamente U$D 20.000 y con una licencia anual que cuesta U$D 7.000 renovar. **https://www.clarin.com/policiales/detectives-telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html**

15 / Ibid

16 / Clarín. "Detectives de teléfonos: secretos del sistema que abre los celulares y resuelve las causas más complejas", Noviembrel 2020 **https://web.archive.org/web/20201114090956/https://www.clarin.com/policiales/detectives -telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html**

17 / La información aquí mencionada surge de la investigación realizada para el informe "Tecnologías de Vigilancia en Argentina", 2021, disponible en **https://adc.org.ar/wp-content/uploads/2021/12/ADC-Tecnologias-de-vigilancia-en-Argentina.pdf**

18 / Clarín. "Detectives de teléfonos: secretos del sistema que abre los celulares y resuelve las causas más complejas". Noviembre 2020 **https://www.clarin.com/policiales/detectives-telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html**

19 / Web oficial de Cellebrite **https://www.cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/** y **http://web.archive.org/web/20211222131350/https://www.cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/**

20 / Expediente Nº 37/105-0815-CDI19. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwbeNKAPenXR8IR3ih5YSXR79Wk8x7mmrwOCg9|4XRUnx0kCgm3oU8Rx5zyjpByUn|6t4HsX9ox3IM|fHZHcPGbahOwPe58NWP7IaFH5JcDkQ==

21 / Ibid

22 / Dirección de Criminalística y Estudios Forenses. "ADQUISICIÓN DE SOFTWARE UFED 4PC PARA LA DIRECCIÓN DE CRIMINALÍSTICA Y ESTUDIOS FORENSES". Expediente Nº 37/105-0041-LPU19. Julio del 2018 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy5xycgc2RiGO0seBx38Zrkqrf44NYcUHOQX WAZSx|FbiACHf8VyMdhxK5ugYZKg/ha7EWhWl7fjuQEoJmuXixefeg9/er7CV2Q|P|HNndQKg==

23 / Dirección de Criminalística y Estudios Forenses. "SERVICIO DE RENOVACIÓN Y ACTUALIZACIÓN DE LICENCIAS DE SOFTWARE FORENSE UFEC TOUCH I HACIA UFED 4PC". Expediente Nº 37/105-0422-CDI20. Marzo del 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyrV/4BRRj7a9qf3aG8azk|h3K/KAn7jb/h6aP Dkgsy3caJklV5dh/l98fSQHDGyecUZqnGVTQz3UXLzeKrU0hskSjg8CnHW3bp5dO0tjSzbg==

24 / Cellebrite. UFED Ultimate. https://www.cellebrite.com/en/ufed-ultimate/

25 / Policía de Seguridad Aeroportuaria. "Renovación de licencias y mejoramiento de equipos UFED 4PC y UFED TOUCH, por Exclusividad". Expediente Nº 279-0027-CDI20. Noviembre del 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy3iTxQqkwwChRpn2XPxXCSk5uij|LSdq2D mF5S3lGnqlsUbG2uGBeZPrbB8BhNUcLFrujs6LrFUaU3GDH8dDYrJv/eOuj/ve1TCcZ2AXWpaw==

26 / Telam, 2020, "Estiman que los celulares de los rugbiers aportarán 4 terabytes de información" https://www.telam.com.ar/notas/202001/427923-pericias-telefonos-celulares-rugbiers-crimen-fernando-baez-sosa-villa-gesell.html

27 / Fiscalía Federal N1 de Bahia Blanda, "Disponen medidas para investigar el contexto que rodeó al hallazgo del cuerpo en Villarino Viejo" https://www.fiscales.gob.ar/violencia-institucional/disponen-medidas-para-investigar-el-contexto-que-rodeo-al-hallazgo-del-cuerpo-en-villarino-viejo/

28 / Radio Bicentenario, 2020. "Finalmente pudieron desbloquear los celulares de los diez rugbiers", **https://www.radiobicentenario.com.ar/nota/policia-federal/8389/finalmente-pudieron-desbloquear-celulares-diez-rugbiers.html**

29 / Memoria Anual 2020, Ministerio de Seguridad, Prefectura Naval Argentina, pag. 321 **https://www.argentina.gob.ar/sites/default/files/2020/12/titulo_ii.pdf**

30 / Ministerio de Justicia y Derechos Humanos. "Laboratorios Regionales de Investigación Forense". Agosto 2014 **http://www.saij.gob.ar/docs-f/ediciones/libros/Laboratorios_Regionales_de_Invest._Forense.pdf**

31 / El Ministerio de Justicia invierte $125 millones para que los Ministerios Públicos Fiscales y de la Defensa mejoren los laboratorios de investigación forense

32 / El Entre Rios, "Dispositivos UFED, el nuevo equipamiento con el que cuenta la policía de Concordia y la Gendarmería en Paraná", **https://www.elentrerios.com/actualidad/dispositivos-ufed-el-nuevo-equipamiento-con-elque-cuenta-la-polica-de-concordia-y-la-gendarmera-en-paran.htm**

33 / Ministerio de Justicia y Derechos Humanos. "Laboratorios Regionales de Investigación Forense". Agosto del 2014 **http://www.saij.gob.ar/docs-f/ediciones/libros/Laboratorios_Regionales_de_Invest._Forense.pdf**

34 / "Tecnologías de Vigilancia en Argentina", ADC, 2021 **https://adc.org.ar/wp-content/uploads/2021/12/ADC-Tecnologias-de-vigilancia-en-Argentina.pdf - Ministerio Público, provincia de Salta. Expediente N° 130-17.933/17**

35 / Ministerio Público Fiscal de la Provincia de Salta, "Las fiscalías del Norte contarán con nuevo equipamiento" 3 de abril de 2019

36 / Ministerio Público Fiscal de la Provincia de Salta **https://www.fiscalespenalesalta.gob.ar/?s=ufed**

37 / Licitación Pública 12/21, Boletín Oficial de la Provincia de Salta **https://boletin-oficialsalta.gob.ar/instrumento.php?cXdlcnR5dGFibGE9QXwxMDAwODc4NjUmZG-F0YT0yMTA2M3wyMDIxcXdlcnR5**

38 / Colegio de Gobierno por Res. Nº 20342 - LICITACIÓN PÚBLICA Nº 12/2021 "RENOVACIÓN DE 1(UNA) LICENCIA DE SOFTWARE UFED ULTIMATE TOUCH2 Y 1(UNA) LICENCIA DE SOFTWARE UFED CLOUD"**https://www.mpublico.gov.ar/Contratacion/Licitacion-Publica-N-122021-%E2%80%9CRenovacion-de-1(una)-licencia-de-software-UFED-ULTIMATE-TOUCH2-y-1(una)-licencia-de-software-UFED-CLOUD%E2%80%9D._2825**

39 / Diario 21, Marzo 2021, "Como se perita un telefono celular en el gabinete cientifico del Chacho" **http://www.diario21.tv/notix2/movil2/noticia/151989_video---coacutemo-se-perita-un-teleacutefono-celular-en-el-gabinete-cientiacutefico-del-chaco.html**

40 / Prensa Justicia Chaco, Enero 2018, "La Justicia dispondrá de equipos de alta tecnología para las pericias forenses" **http://prensa.justiciachaco.gov.ar/node/2759**

41 / Ministerio Publico de Santa Fe, Memoria Institucional 2018, **http://www.mpfsde.gob.ar/wp-content/uploads/2020/09/Memoria-Institucional-MPF-Sgo.-17-18.pdf**

42 / Ministerio Público Fiscal de Chubut, Marzo 2018, "Reglas de coordinación de actividades entre el equipo tecnico multidisiplinario y la Agencia Policial para la Investigación de Hechos Delictivos" **http://www.mpfchubut.gov.ar/images/stories/comunicadores/Comodoro_Rivadavia/PGA_004946_Reglas_mnimas_ETM_policia.pdf**

43 / Ministerio Público de la Provincia de Buenos Aires, Informe de Gestión 2020, **https://www.mpba.gob.ar/files/content/Informe%20de%20Gestion%202020.pdf**

44 / Ministerio Público de la Provincia de Buenos Aires, "La Fiscalía General de Bahia Blanca incorpora Software UFED" **https://www.mpba.gov.ar/novedad/681**

45 / Licitación Pública de Etapa Única N° 2900- 1311-LPU20 **https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJYSGC-SSGA-5-21-ANX.pdf** Detalles tecnicos: **https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJYSGC-SSGA-5-21-ANX-1.pdf**

46 / Resolución FGAF 230/2020 disponible en **https://mpfciudad.gob.ar/compras/search**

47 / LICITACIÓN PÚBLICA 02-2021 REN1: Renovación Licencias 7 licencias UFED 4PC y 2 licencias KIOSK INFIELD para el uso del Cuerpo de Investigaciones Judiciales del Ministerio Público Fiscal de la Ciudad autónoma de buenos Aires, Adjudicada por RESOLUCIÓN FGAG 178/2021- ADJUDICACIÓN

48 / Resolución FGAG 178/2021 disponible en **https://mpfciudad.gob.ar/compras/search**

49 / Disposición UOA 106-2019 disponible en **https://mpfciudad.gob.ar/storage/archivos/Disposici%C3%B3n%20UOA%20106-2019.pdf**

50 / Gobierno de la Ciudad Autónoma de Buenos Aires. Disposición N° 65/UOA/19 Julio del 2019. **https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PJ-DIS-MPF-UOA-65-19-5660.pdf**

51 / Ministerio Público Fiscal de la Provincia de Buenos Aires. Disposición UOA N° 45/2017. Septiembre del 2017. **https://mpfciudad.gob.ar/storage/archivos/Disposici%C3%B3n%20UOA%20N%C2%BA%2045-17%20AI%2030-00036938%20A djudicacion%20SECURITY%20TEAM%20NETWORK%20S.A.%20-Ufed%20Cloud-.pdf**

52 / Ministerio Público de la Acusación de la Provincia de Santa Fe. Expediente Nº FG-000303-2020. Agosto del 2020 **https://www.mpa.santafe.gov.ar/regulations_files/5f328fd04126a_Resoluci%C3%B3n%20N%C2%B0%20274.pdf**

53 / La información se obtuvo de la investigación de la ADC realizada para el informe “Tecnologías de Vigilancia en Argentina”, 2021, disponible en **https://adc.org.ar/wp-content/uploads/2021/12/ADC-Tecnologias-de-vigilancia-en-Argentina.pdf**

54 / Compulsa Abreviada 25/2015 publicada en el boletín oficial **https://boletin-oficial.cba.gov.ar/wp-content/4p96humuzp/2015/11/181115_bocba_4ssvU1Gn.pdf - Detalle tecnico https://silo.tips/download/compulsa-abreviada-n-25-15-pliego-de-condiciones-generales-y-especificaciones-te**

55 / Ministerio Público Fiscal de Cordoba, "Incorporación de tecnología en el Ministerio Público Fiscal" **http://www.mpfcordoba.gob.ar/incorporacion-de-tecnologia-en-el-mpf/**

56 / Clarín, Noviembre 2020, "Detectives de teléfonos: secretos del sistema que abre los celulares y resuelve las causas más complejas" **https://web.archive.org/web/20201114090956/https://www.clarin.com/policiales/detectives -telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html**

57 / Página oficial de MSAB **https://www.msab.com/about-us/**

58 / Página oficial de MSAB, descripción del producto XRY Logical **https://www.msab.com/wp-content/uploads/2021/11/XRY_Logical_EN.pdf**

59 / Página oficial de MSAB, descripción del producto XRY Physical **https://www.msab.com/wp-content/uploads/2021/10/XRY_Physical_US.pdf**

60 / Página oficial de MSAB, descripción del producto XRY Cloud **https://www.msab.com/wp-content/uploads/2021/10/XRY_Cloud_EN.pdf**

61 / Página oficial de MSAB **https://www.msab.com/about-us/**

62 / La información surge de una compra realizada por el gobierno de Puerto Rico en el año 2020, disponible en **https://transicion2020.pr.gov/Agencias/189/Informe%20Inventario%20Propiedad/Informe%20de%20Inventario%20de%20Propiedad%20-%20NCF.pdf**

63 / Descripción de MSAB en el portal Security Weekly, 01.10.2015 **https://www.sc-magazine.com/product-test/-/msab-xry-office**

64 / Ministerio Público Fiscal de la Nación, Informe Anual 2016, Pag. 72. **https://www.mpf.gob.ar/wp-content/uploads/2017/05/Informe-Anual-2016.pdf**

65 / Ministerio Público de Rio Negro, Memoria Institucional 2017, Pag. 75 https://ministeriopublico.jusrionegro.gov.ar/content/memorias/memoria_2017.pdf

66 / Prensa Justicia Chaco, Enero 2018, "'La Justicia dispondrá de equipos de alta tecnología para las pericias forenses" http://prensa.justiciachaco.gov.ar/node/2759

67 / Ministerio Público de la Provincia de Buenos Aires, Informe de Gestión 2019, Pag. 226 https://www.mpba.gov.ar/files/content/Informe%20de%20Gestion%202019.pdf

68 / Ministerio Público Fiscal de Santiago del Estero, Memoria Institucional 2014, http://www.mpfsde.gob.ar/wp-content/uploads/2017/11/15-06-11Memoria-2014-FINAL.pdf

69 / Ministerio Público Fiscal de Santiago del Estero, Memoria Institucional 2015, Pag, 73 http://www.mpfsde.gob.ar/wp-content/uploads/2017/11/Memoria-2015-FINAL.pdf

70 / Ministerio Público Fiscal de Santiago del Estero, Memoria Institucional 2018 http://www.mpfsde.gob.ar/wp-content/uploads/2020/09/Memoria-Institucional-MPF-Sgo.-17-18.pdf

71 / Pliego de bases y condiciones disponible en http://onc-ftp1.argentinacompra.gov.ar/0030/000/050000012018000000/CNV-000739256001.pdf y en https://www.argentinalicitaciones.com/adquisicion-de-siete-7-dispositivos-para-extraccion-de-datos-de-aparatos-de-telefonia-celular-movil-marca-xry-version-complete-con-licencia-por-treinta-y-seis-36-meses-lct20532.html

72 / Página oficial de Magnet Forensics, https://www.magnetforensics.com

73 / Página oficial de Magnet Forensics, descripción del producto Magnet Axiom https://www.magnetforensics.com/products/magnet-axiom/

74 / Página oficial de Magnet Forensics, https://www.magnetforensics.com

75 / Disposición OAF 81/2020 disponible en https://mpfciudad.gob.ar/compras/search

76 / Disposición UOA 63/2019 disponible en **https://mpfciudad.gob.ar/compras/search**

77 / Pedido de Acceso a la Información Pública efectuado por ADC en octubre del 2021 bajo el número de expediente N EX-2021-23272451-GCABA-DGSOCAI-21

78 / Ministerio Público de Santa Fe, Informe de Gestión, **https://mpa.santafe.gov.ar/mediafiles/nw5f6352fde34f4_58_Informe%20de%20Gesti%C3%B3n%20de%20la%20Fiscal%C3%ADa%20General%20%7C%202018-2019.pdf**

79 / RESOLUCIÓN Nº 2137- MPA /2020.- SAN SALVADOR DE JUJUY, 29 DIC. 2020 **http://boletinoficial.jujuy.gob.ar/?p=213545**

80 / El uso de software abierto para el análisis de la evidencia digital por Gustavo PResman y Pablo A. Palazzi, disponible en **https://udesa.edu.ar/sites/default/files/revistardyntnro1.pdf.**

81 / En contraposición, se encuentra el software libre o de código abierto que permite acceder, compartir y modificar el código fuente en favor de la comunidad

82 / "UNA CUESTIÓN DE CÓDIGOS: LA UTILIZACIÓN DE ALGORITMOS SECRETOS EN LA JUSTICIA PENAL" Polansky Jonathan A. (2020). Garantías constitucionales del procedimiento penal en entorno digital. (1ª Edición). Hammurabi. **https://biblioteca.hammurabidigital.com.ar/reader/garantias-constitucionales-en-entorno-digital?location=99**

83 / Polansky Jonathan A. (2020). Garantías constitucionales del procedimiento penal en entorno digital. (1ª Edición). Hammurabi. **https://biblioteca.hammurabidigital.com.ar/reader/garantias-constitucionales-en-entorno-digital?location=102**

84 / En Argentina no existe un desarrollo jurisprudencial acabado sobre el tema, sin embargo, en EEUU se ha abordado la cuestión, entre otros en el caso sobre programas de detección de ADN TrueAllele analizado en el caso "Commonwealth of Pennsylvania v. Michael Robinson",caso CC 201307777, resuelto por la Corte del Condado de Allegheny del Estado de Pensilvania en EEUU **https://www.prisonlegalnews.org/news/2017/mar/9/defense-attorneys-seek-access-dna-matching-softwares-source-code/**

85 / Ibid

86 / Signal, "Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective", 21.04.2021 **https://signal.org/blog/cellebrite-vulnerabilities/**

87 / https://signal.org/blog/cellebrite-vulnerabilities/

88 / Vice, "Lawyer Asks For New Trial After Cellebrite Vulnerability Discovery", 27.04.2021 **https://www.vice.com/en/article/5dbpyq/lawyer-new-trial-cellebrite-signal-vulnerability**

89 / El uso de software abierto para el análisis de la evidencia digital por Gustavo PResman y Pablo A. Palazzi, disponible en **https://udesa.edu.ar/sites/default/files/revistardyntnro1.pdf.**

90 / ADC, "El Debido Proceso Digital", 2019 **https://adc.org.ar/wp-content/uploads/2019/12/El-debido-proceso-digital-12-2019-V1.pdf**

91 / Existen discusiones muy relevantes acerca de cómo debe realizarse el análisis de la información y en qué casos se puede utilizar información encontrada que no sea parte del objeto investigado. La discusión acerca de la aplicación de la doctrina de "Plain View" se encuentra parcialmente analizada en el libro Garantías constitucionales del procedimiento penal en el entorno digital de Polansky, Jonathan A. (2020)

92 / Polansky Jonathan A. (2020). Garantías constitucionales del procedimiento penal en entorno digital. (1ª Edición). Hammurabi. **https://biblioteca.hammurabidigital.com.ar/reader/garantias-constitucionales-en-entorno-digital?location=103**

93 / ADC, "¿Cómo implementar la debida diligencia en Derechos Humanos en el desarrollo de Tecnología? El impacto en la Privacidad", 2020 **https://adc.org.ar/wp-content/uploads/2020/10/Guia-Debida-Diligencia-DDHH-Analisis-de-Impacto-en-Privacidad.pdf**

adc.org.ar