Investigar para proteger

GUÍA TÉCNICA SOBRE DELITOS EN ENTORNOS DIGITALES QUE AFECTAN A NIÑAS, NIÑOS Y ADOLESCENTES EN LA ARGENTINA

unicef | para cada infancia

CRÉDITOS

Dirección editorial:
Alejandro Morlachetti, Especialista de Protección de Derechos, UNICEF Argentina.

Coordinación general y revisión de contenidos:
María Dinard, Oficial de Protección de Derechos, UNICEF Argentina.

Autoría:
Daniela Dupuy, Directora del Observatorio de Cibercrimen y Evidencia Digital (OCEDIC) de la Universidad Austral y Fiscal especializada en Cibercrimen de la Ciudad Autónoma de Buenos Aires.

Colaboración:
Ana Zolezzi Mir, Team Leader del Observatorio de Cibercrimen y Evidencia Digital (OCEDIC) de la Universidad Austral.

INVESTIGAR PARA PROTEGER. Guía técnica sobre delitos en entornos digitales que afectan a niñas, niños y adolescentes en la Argentina. Primera edición. Mayo de 2026.

Diseño y diagramación: Gomo Studio
Edición y corrección: Estudio REC

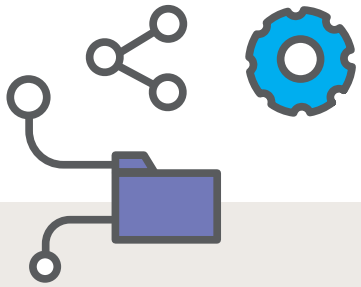
UNICEF Argentina buenosaires@unicef.org
www.unicef.org/argentina

Investigar para proteger

GUÍA TÉCNICA SOBRE DELITOS EN ENTORNOS DIGITALES QUE AFECTAN A NIÑAS, NIÑOS Y ADOLESCENTES EN LA ARGENTINA

unicef | para cada infancia

Índice



Introducción 5

Los objetivos de esta guía 6

Primera parte 7

Sobre el ciberespacio y los delitos 8
¿Por qué internet revolucionó y facilitó el mercado de la explotación sexual contra NNyA? 9
Qué dicen los datos 10

Investigar delitos digitales: nuevos desafíos para la Justicia 12

Marco normativo 14
Tratados internacionales 14
Normativa nacional 16

Segunda parte 18

Cómo proceder ante delitos en entornos digitales que afectan a NNyA 19

Tres pasos fundamentales para una investigación eficiente 21
Paso 1. Identificar y determinar el hecho a investigar subsumible en una figura legal 21
Paso 2. Resguardar y preservar de la evidencia digital 23
Paso 3. Identificar al sospechoso e investigar la maniobra delictiva 29

Obtención y preservación de evidencia digital: protocolo de buenas prácticas 43
Cadena de custodia 45
Requisitos de admisibilidad de la evidencia digital 51

Consideraciones y recomendaciones 53

Glosario 55

Siglas 59

Bibliografía 61

Introducción

Internet ha impactado en nuestras vidas. Si bien el desarrollo tecnológico es una herramienta favorable para el alcance global de la comunicación, también es cierto que se ha convertido en un facilitador de muchas actividades delictivas. Quienes cometen delitos contra los niños, niñas y adolescentes (NNyA) mediante tecnologías digitales pueden acosarlos con fines sexuales (*grooming*) y consumir, demandar, producir, compartir, ofrecer y comercializar imágenes de abuso sexual (explotación sexual de NNyA) en entornos digitales (internet y teléfonos celulares). Internet les permite hacerlo de una manera fácil, económica, con bajo riesgo, sin obstáculos de límites geográficos y desde el anonimato.

Para que esto ocurra, el abuso sexual de NNyA será muchas veces el primer paso, ya que permitirá fotografiarlos y filmarlos durante el acto sexual, para luego eternizar la violación a su integridad sexual a través del intercambio y la difusión de esos archivos en una red nacional o internacional, dejando una huella para siempre en sus vidas.

Quienes abusan de NNyA y registran a través de cámaras de video, fotos o celulares esa actividad para luego vender o intercambiar esas imágenes son explotadores sexuales de NNyA, y cuando alguien paga por aquellas o las descarga también participa de la explotación, formando parte del circuito delictivo.

El advenimiento de internet y de la telefonía móvil ha facilitado las descargas e intercambios de material de explotación sexual de NNyA, generando que su producción y posterior venta se convierta en un negocio lucrativo a nivel mundial.

En consecuencia, se debe trabajar profundamente en una política pública clara, específica y global que, a través de la cooperación internacional, termine con estos delitos. Ello debe estar acompañado por legislaciones de forma y de fondo adaptadas a las nuevas tecnologías. Es fundamental, además, capacitar a los operadores del sistema de justicia (jueces, fiscales, fuerzas de la ley) para que logren un conocimiento acabado y minucioso sobre los pasos y las herramientas con los que se investigan y resuelven estos delitos, incluso aquellos que ocurren en entornos digitales transnacionales.

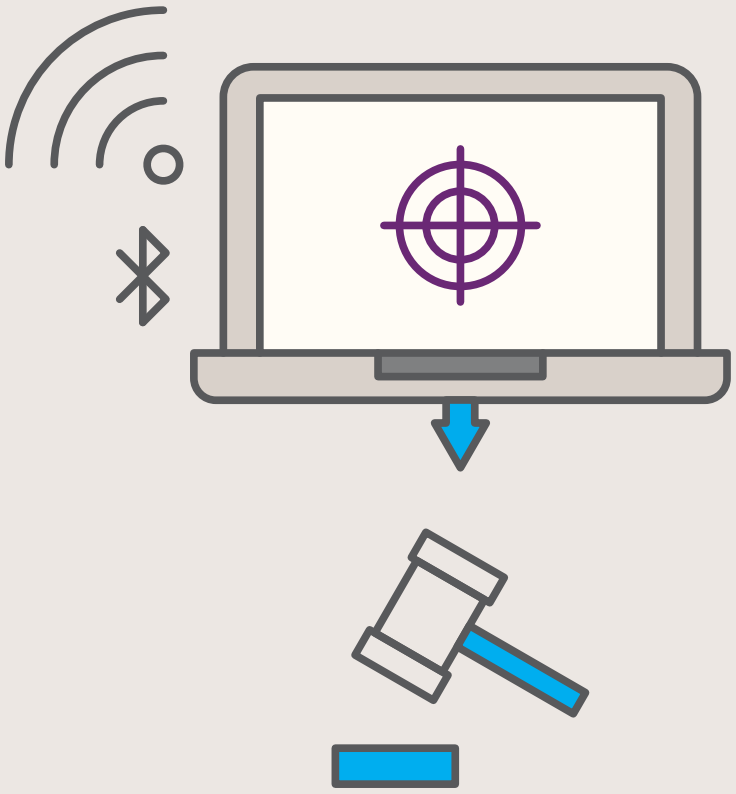
Los objetivos de esta guía

El propósito de esta guía destinada a quienes trabajan en el ámbito de la Justicia argentina es explicar los pasos a seguir y las herramientas a utilizar para llevar adelante la investigación de casos de *grooming* y explotación sexual de NNyA en entornos digitales, junto con sus derivaciones. Se incluye la trazabilidad completa y el tratamiento de la evidencia digital en los delitos en los que NNyA son víctimas.

Dado que en el país no hay lineamientos concretos ni tampoco regulación sobre la recolección y valoración de la evidencia digital, esperamos que esta guía resulte de relevancia.

Además, se sistematizan los hallazgos y las últimas tendencias en la investigación penal de delitos cometidos en entornos digitales. En ese sentido, otro de los objetivos de esta guía es reflexionar sobre los nuevos desafíos que surgen de los delitos cometidos en entornos digitales que afectan a niños, niñas y adolescentes.

Primera parte



Sobre el ciberespacio y los delitos

Una forma de concebir al ciberespacio es entenderlo como un nuevo espacio de intercomunicación transnacional e universal que está sujeto a evolución permanente. En ese sentido, la transnacionalidad, la fugacidad, la volatilidad de sus contenidos y las acciones de quienes intervienen en una comunidad virtual son características importantes que impactan en materia de derecho penal. Ello obliga no solo a una revisión del derecho penal y procesal penal, sino también de la teoría criminológica, que debe adaptar sus conceptos.

Según Miró Linares (2012), el ciberespacio no cambia los caracteres esenciales que hacen que a determinados eventos se les pueda seguir denominando crímenes, pero sí modifica los parámetros de espacio-tiempo en los que el crimen tiene lugar.

Desde el punto de vista del ciberagresor, su campo de oportunidad es muy amplio en el ciberespacio debido a que no es necesario que exista una cercanía entre agresor y víctima para que se concrete el delito, tal como se requiere en el espacio físico. Es decir que, en internet, la distancia física deja de ser una barrera para la comisión de delitos.

Lo expuesto, sumado a la transnacionalidad como característica fundamental de esta modalidad delictiva, el anonimato del agresor y el aumento masivo de personas que interactúan en redes sociales, dificultan en el ciberespacio la existencia y actuación de elementos eficaces de protección de la víctima, frente a un agresor que percibe menos obstáculos para su accionar y, por ende, siente menos riesgo de ser individualizado por los investigadores.

Ello explica un aumento en el número de agresores y, por consiguiente, de víctimas incapaces de ser tuteladas por el Estado.

En ese sentido, vale destacar que un hito importante en la regulación de las pruebas digitales es la Convención de las Naciones Unidas contra la Ciberdelincuencia Cibernética, de fines de 2024[1], que establece un marco global para la cooperación transfronteriza jurídica mutua y las garantías de los derechos humanos[2].

¿Por qué internet revolucionó y facilitó el mercado de la explotación sexual de NNyA?

La explotación sexual de NNyA es un problema internacional que se ha ramificado con el avance de las nuevas tecnologías, que no solo permiten y facilitan la comisión de esta conducta delictiva, sino que tornan insuficientes los programas de acción de los diferentes países del mundo para combatirla.

La eclosión de internet ha revolucionado y facilitado el mercado de la explotación sexual de NNyA en línea por varias razones:

- Disponibilidad económica de los usuarios para acceder a los equipos informáticos que posibilitan la captación y obtención de material de abuso sexual de NNyA.
- Abundancia de material de abuso sexual de NNyA que circula por la red y facilita la interrelación entre un enorme número de aficionados, permitiendo un intercambio constante de fotografías, videos, películas, producciones, etc.
- Simplicidad para descargar y compartir archivos a cero costo económico, pues las técnicas de producción e introducción de dicho material en la red se han multiplicado. Por ejemplo, conversaciones interactivas por WhatsApp y Telegram, etc., que permiten fácilmente poner a disposición videos y fotografías.
- La ventaja de permanecer en el anonimato. Compartir dichos archivos detrás de la pantalla fomenta y alienta altamente el intercambio, facilitación y distribución del material, pues se desconoce el origen de la transmisión de los datos. El usuario puede enmascararse en identidades ficticias o de imposible identificación y difundir contenidos a otro país, dificultando rastrear el origen desde donde se subió efectivamente el material de abuso sexual de NNyA.
- La posibilidad de conectar, con mayor practicidad, con NNyA a través de internet, ya que las redes sociales son una herramienta de comunicación natural y permanente entre ellos.
- La figura del vendedor de material de abuso sexual de NNyA fue sustituida por la de consumidores que se asocian sin ánimo de lucro, bajando, subiendo y facilitando archivos, rápidamente y ayudados por las técnicas avanzadas de la tecnología P2P (redes de intercambio de archivos entre pares; red *peer to peer*).
- La existencia de manuales de ayuda a pedófilos que permiten intercambiar información para obtener material de abuso sexual de NNyA y brindan consejos y advertencias para permanecer en el anonimato y no ser descubiertos por la Justicia.

1. Para más información, visitar: https://www.unods.org/unodc/es/cybercrime/convention/text/convention-full-text-html
2. Para más información, ver las Directrices para fiscales sobre la recopilación de las pruebas digitales de la UNESCO y la International Association of Prosecutors (pág. 4).

Distintas finalidades

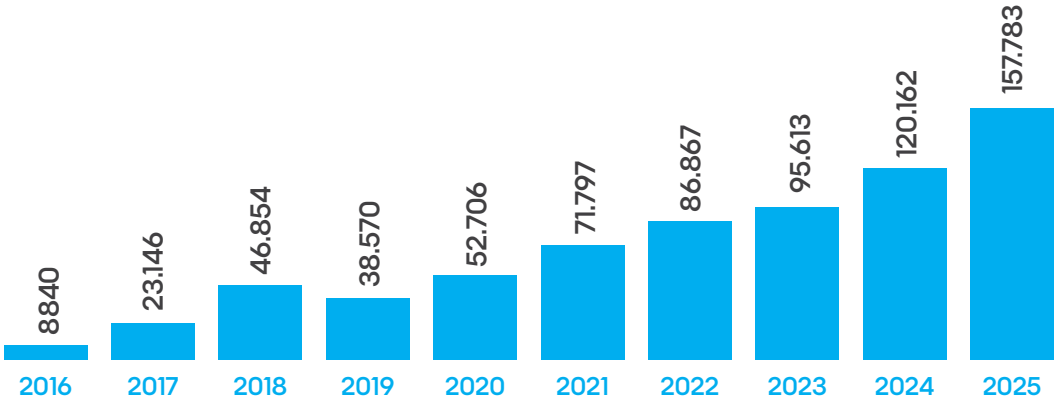
La distribución e intercambio de material sexual de NNyA no se reduce en todos los casos a una finalidad comercial o de lucro, sino a satisfacer las inclinaciones de los consumidores, con la consiguiente creación de redes internacionales de intercambio de material de abuso sexual. Esto genera espacios que facilitan e incrementan la colección de fotografías y videos que los delincuentes suelen seleccionar y archivar en diferentes carpetas, etiquetadas de acuerdo a la edad, el sexo, el color de pelo de niños y niñas, desde una edad muy temprana —bebés de pocos meses— hasta pasada la adolescencia.

Qué dicen los datos

A nivel internacional, en 2024 se registraron en el National Centre for Missing and Exploited Children 20,5 millones de reportes o denuncias. Ello representa 33.130.449 videos, 28.004.236 imágenes y 1.858.174 archivos similares que muestran bebés, niños y niñas de corta edad y adolescentes siendo abusados sexualmente por adultos. En total suman 62.992.859 archivos que implican casi 63 millones de NNyA víctimas de esos delitos contra la integridad sexual.

En la Argentina, el Ministerio Público Fiscal (MPF) de la Ciudad Autónoma de Buenos Aires (CABA) es la entidad que recibe desde NCMEC los reportes de los sospechosos que habrían acosado a un NNyA desde nuestro país y producido o comercializado las imágenes o videos de naturaleza sexual en redes internacionales de explotación sexual de NNyA. Luego, al establecer la ubicación del eventual autor de estos delitos, se remite la denuncia a la provincia correspondiente para su urgente investigación. En 2025, ingresaron a nuestro país 157.783 denuncias, lo que implica más de 240.000 archivos y más de 437.390 NNyA víctimas.

Figura 1. Ingreso de reportes desde el NCMEC a la Argentina, 2016-2025



Fuente: National Center for Missing and Exploited Children.

El NCMEC y la CyberTipline

El NCMEC es una organización sin fines de lucro con sede en los Estados Unidos que ha recibido apoyo del Congreso de ese país con el fin de construir una respuesta internacional coordinada e intercambiar información respecto a la problemática de los niños desaparecidos y explotados sexualmente. Esta ONG ha obtenido autorización para establecer el sistema CyberTipline, que proporciona un mecanismo centralizado en el que los proveedores de servicios de internet (Facebook, Microsoft, Twitter, TikTok, etc.) le reportan actividades sospechosas relacionadas a la explotación sexual de NNyA, pues una ley federal así lo exige.

Investigar delitos digitales: nuevos desafíos para la Justicia

En un mundo cada vez más digitalizado, en el que las posibilidades para cometer delitos se encuentran facilitadas por herramientas disruptivas y al alcance inmediato de los ciberdelincuentes, uno de los mayores desafíos representa cómo investigar en un contexto diferente y poco regulado sin afectar derechos fundamentales y garantías constitucionales.

Se parte de la base de que la evidencia digital es volátil e implica una lógica diferente cuando se requiere su preservación, extracción, análisis y presentación en el marco de una investigación. Esas particularidades la distinguen de la incautación de la prueba física aplicada en las investigaciones tradicionales.

En ese sentido, el tiempo es su peor enemigo: entre que el hecho se comete en entornos digitales, se descubre el acto y la prueba se entrega a las autoridades competentes para su correspondiente investigación, es posible que cuando se requiera la evidencia digital esta ya no exista, haya sido borrada.

Además, una de las características fundamentales del entorno virtual es la ubicuidad: el autor del hecho puede encontrarse en un país o varios, la víctima en otro, y la evidencia digital que se necesita para comprobar uno de los aspectos de la teoría del caso de cualquiera de las partes puede estar alojada en un servidor en otro país, o bien los datos pueden estar fragmentados en diferentes servidores de distintos países. Se observa, entonces, que la falta de límites o fronteras para cometer el delito debilita el tradicional principio de territorialidad y soberanía nacional que siempre hemos estudiado.

En este escenario aparece un actor fundamental: el sector privado. Los proveedores de servicios de internet (en adelante, los ISP, por sus siglas en inglés)[3] tienen en su poder la información básica y necesaria de los usuarios que permite iniciar un caso, identificar a quién o a quiénes infringen la norma y eventualmente atribuirles responsabilidad penal.

Lo expuesto requiere profundizar los mecanismos de cooperación internacional entre los Estados y también entre los Estados y los ISP.

Además, los Estados deben estar a la altura tecnológica para responder ante esos delitos, debiendo lograr un equilibrio entre la persecución penal y los derechos fundamentales de los ciudadanos. También, se necesitan jueces que incorporen los conocimientos tecnológicos aplicados en el paso a paso de una investigación que afecta a NNyA, para que sus decisiones sean de la mayor calidad posible.

En conclusión, y como lo exige el Convenio de Budapest a los Estados parte[4], una de las obligaciones es que las normas procesales sean adaptadas a los delitos cometidos en entornos digitales, incluyendo medidas de preservación y recolección de evidencia digital. Y ello se deriva en una correcta aplicación del derecho por parte de los operadores del sistema, que necesitan profundizar sus conocimientos tradicionales y fortalecerlos con las nuevas tendencias tecnológicas que tanto afectan a la infancia.

A los desafíos señalados se agrega una carencia legislativa procesal en la Argentina, como así también en la mayoría de los países de la región, en cuanto a la regulación de la recolección y valoración de la evidencia digital en el sistema penal, y de los medios de investigación modernos adaptados a las nuevas tecnologías.

3. ISP son las siglas en inglés de *internet service provider*: una compañía que proporciona acceso a internet. Se trata de toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de un sistema informático, como así también cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios. —conf. art. 1.c del Convenio sobre la Ciberdelincuencia—.
4. Por medio de la Ley 27.411 (B.O. 15/12/2017), la Argentina adhirió al Convenio sobre la Ciberdelincuencia de Budapest del 23 de noviembre de 2001, vigente en el país desde el 1 de octubre de 2018.

Marco normativo

Son numerosos los tratados y documentos internacionales que reflejan el acuerdo entre los países para luchar contra el abuso y la explotación sexual de NNyA. También se requiere una eficiente coordinación nacional e internacional y la creación de políticas públicas por medio de la aprobación de legislaciones uniformes.

Importa destacar que la diferencia entre las leyes de distintos países debilita la posición que se debe tener para luchar contra la explotación sexual de NNyA, permitiendo que los abusadores concentren sus esfuerzos en países en los que saben que no serán criminalizados pues no se persiguen penalmente estos delitos.

Cumplir con los estándares legales internacionales es el comienzo del camino, seguido de la implementación de la legislación nacional y de la creación de programas y políticas públicas relacionadas al abuso, explotación y violencia contra NNyA.

Tratados y convenciones internacionales

Convención Internacional sobre los Derechos del Niño

Fue adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989. La Argentina la ratificó en 1990 y en 1994 le otorgó rango constitucional. Reconoce que los niños, niñas y adolescentes son titulares de derechos y es el primer instrumento a nivel internacional que establece todos los derechos humanos que protegen a la niñez y la adolescencia. Regula la obligación de los países de adecuar sus legislaciones internas para defender los preceptos que establece (art. 3).

El artículo 34 hace expresa referencia al material de abuso sexual de NNyA mediante el uso de las tecnologías de la información y la comunicación, destacando el compromiso por la protección de los niños[5].

Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía[6]

Entró en vigor el 18 de enero de 2002, refiriéndose específicamente a la explotación sexual de NNyA, y definiéndola como "cualquier representación, por cualquier medio, de un niño efectuando actividades sexualmente explícitas reales o simuladas, o cualquier representación de las partes sexuales del niño con fines principalmente sexuales".

Es de destacar que en el artículo 3 (4) aborda el tema de la responsabilidad de las personas jurídicas, e incentiva a cada Estado Parte para que haga efectiva dicha responsabilidad por delitos específicos relacionados con la pornografía infantil. Este artículo refleja la noción de que un enfoque integral requiere la participación de la industria.

Convención del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual (Convenio de Lanzarote)

Firmado el 25 de octubre de 2007, este acuerdo se enfoca en asegurar lo que resulte mejor para los intereses de los niños mediante la prevención del abuso y la explotación sexual, la protección y ayuda para las víctimas, el castigo a los delincuentes y la promoción de leyes de cooperación nacional e internacional entre los cuerpos policiales[7].

Convenio sobre la Ciberdelincuencia (Convenio de Budapest)

El Consejo de Europa lo estableció el 23 de noviembre de 2001 con la esperanza de implementar un enfoque cooperativo y uniforme para la persecución del delito informático. En 2017, por medio de la Ley 27.411, la Argentina adhirió y está vigente desde octubre de 2018.

5. Que los Estados Partes se comprometen a proteger al niño contra todas las formas de explotación y abuso sexual y tomarán todas las medidas que sean necesarias para impedir:
(a) La incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal;
(b) La explotación del niño en la prostitución u otras prácticas sexuales ilegales;
(c) La explotación del niño en espectáculos o materiales pornográficos.
6. El artículo 3 (1) exige que los Estados Partes tipifiquen como delito la explotación sexual de NNyA cometida a nivel nacional o internacionalmente efectuada de manera individual o colectiva. El artículo 3 (1) (c) exige que los Estados Partes tipifiquen como delito la posesión simple, sin importar la intención de distribución.
El artículo 7 reconoce el derecho a las víctimas de buscar compensación. Y el 8 establece que los Estados Partes deben de tomar medidas apropiadas para proteger los derechos e intereses de los NNyA víctimas en todas las etapas del proceso penal, siendo la principal consideración, el interés superior del niño.
El artículo 9 establece que los Estados Partes adoptarán o reforzarán y aplicarán leyes, medidas administrativas, políticas y programas sociales destinados a la prevención de los delitos y les darán publicidad. Se prestará particular atención a la protección de los niños que sean especialmente vulnerables a esas prácticas.
También incentiva el fortalecimiento de la cooperación y asistencia internacional y la adopción de legislación extraterritorial, por lo que el artículo 10 (1) aborda el tema de la necesidad de cooperación internacional.
7. Los artículos 4 al 8 establecen las medidas de prevención que deberán adoptar los países que ratifican la Convención, entre ellas, la contratación, formación y sensibilización de las personas que trabajan directamente con niños, educación integral para la niñez, la creación de programas o medidas de intervención preventiva y de evaluación de riesgos y las medidas que se deben tomar para la educación del público en general.
Los artículos 11 al 14 establecen las medidas de protección y asistencia a las víctimas. Estos incluyen la toma de las medidas legislativas o de otro tipo para: asegurar que los profesionales encargados de brindar servicios a NNyA no se vean obstaculizados por las normas de confidencialidad para reportar las sospechas de explotación o abuso sexual; fomentar y apoyar la creación de servicios de información, tales como las líneas de ayuda en internet para proporcionar asesoramiento a las personas que llaman; y ayudar a las víctimas a corto y largo plazo, tanto en su recuperación física como psicosocial.
El artículo 20 (1) requiere que cada parte penalice: producir pornografía infantil, ofrecer o facilitar pornografía infantil, distribuir o transmitir pornografía infantil, procurar pornografía infantil para uno mismo o para otra persona, poseer pornografía infantil y obtener acceso a pornografía infantil de manera intencional y por medio de las tecnologías de la información y la comunicación.
El artículo 20 (2) define a la "pornografía infantil" como "cualquier material que represente visualmente a un niño involucrado en una conducta explícitamente sexual, real o simulada, o cualquier representación de los órganos sexuales de un niño para fines principalmente sexuales".
El artículo 21 (1 y 2) recomienda a los Estados Partes que adopten una legislación que penalice las actividades de quienes contraten u obliguen a un niño a que participe en pornografía infantil o asistan intencionalmente a actos que involucren pornografía infantil.

A través de este convenio, los Estados Partes se comprometieron a intensificar la cooperación internacional de manera reforzada, rápida y eficaz en materia penal y a aplicar, con carácter prioritario, una política penal común con el objeto de proteger a la sociedad frente a la ciberdelincuencia.

El artículo 9[8], referente a la pornografía infantil, tiene como finalidad reforzar las medidas de protección de los menores, incluida su protección contra la explotación sexual, mediante la modernización de las disposiciones del derecho penal con el fin de circunscribir de manera más eficaz la utilización de los sistemas informáticos en relación con la comisión de delitos de índole sexual contra menores. Establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.

Directiva 2011/93/UE del Parlamento Europeo y del Consejo

Fue dictada el 13 de diciembre de 2011 y hace referencia a la lucha contra los abusos y la explotación sexual de menores y la pornografía infantil, ha condicionado e inspirado la reforma que han encarado los países a nivel internacional respecto de los tipos de pornografía infantil[9].

Normativa nacional

Código Penal Argentino

El 21 de marzo de 2018, la Ley 27.436 modificó el artículo 128 del Código Penal para reprimir, con prisión de tres a seis años, a quien produzca, financie, ofrezca, comercie, publique, facilite, divulgue o distribuya, por cualquier medio, toda representación de un menor de 18 años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales. Establece la misma pena para quien organice espectáculos en vivo de representaciones sexuales explícitas en las que participen dichos menores.

Además, determina prisión de cuatro meses a un año para quien a sabiendas tenga en su poder ese tipo de imágenes. Y con prisión de seis meses a dos años a quien tenga en su poder imágenes con fines inequívocos de distribución y/o comercialización. Para quienes faciliten el acceso a espectáculos pornográficos o suministren material pornográfico a menores de 14 años prevé prisión de un mes a tres años.

8. El artículo 9 (1) recomienda que cada Estado Parte tipifique como delito: producir pornografía infantil con el propósito de difundirla a través de sistemas computarizados, ofrecer o facilitar pornografía infantil a través de sistemas computarizados, distribuir o transmitir pornografía infantil a través de sistemas computarizados, adquirir pornografía infantil a través de sistemas computarizados para uno mismo o para otra persona, y poseer pornografía infantil en un sistema computarizado o en un medio de almacenamiento de información computarizado.
El artículo 9 (2) recomienda que la "pornografía infantil" sea definida de manera que incluya "material pornográfico que represente visualmente (...) a un menor involucrado en una conducta explícitamente sexual (...) a una persona que aparente ser menor de edad involucrada en una conducta explícitamente sexual, o (...) imágenes realistas que representen a un menor involucrado en una conducta explícitamente sexual".
El artículo 9 (3) estipula que el término "menor" incluye a toda persona menor de 18 años de edad. Una Parte podrá, sin embargo, exigir un límite de edad más bajo, el cual no deberá ser menor a 16 años.
El artículo 11 exige a los Estados Partes que promulguen la legislación necesaria para enfrentar las tentativas de cometer un delito, así como la ayuda e incitación a cometerlo.
El artículo 12 (1) aborda el tema de la responsabilidad empresarial.
El artículo 13 (1) exige que los Estados Partes adopten medidas legislativas que garanticen que los delitos penalizados "estén sujetos a sanciones efectivas, proporcionales y disuasivas, las cuales incluyan la privación de la libertad".
El artículo 23 aborda el tema de la cooperación internacional.
9. LO 1/2015, de 30 de marzo, España.

Establece, por otro lado, que todas las escalas penales previstas se elevarán en un tercio en su mínimo y en su máximo cuando la víctima sea menor de 13 años.

Respecto al *grooming*, el Código Penal sanciona con prisión de seis meses a cuatro años a quien contacte a un menor de edad por medios digitales con fines de cometer delitos contra su integridad sexual.

Vale destacar que es muy común que, en el marco de la investigación de casos de *grooming* o de explotación sexual de NNyA se detecte la comisión de ambos delitos. Esto obedece a que las imágenes o videos que consigue el *groomer* a través del acoso del NNyA pueden ser luego utilizadas para introducirlos en una red internacional de explotación sexual de NNyA, por ejemplo.

Normativa procesal

Los delitos cometidos con nuevas tecnologías requieren, para ser investigados de manera eficiente, de herramientas forenses y digitales de última generación. Sin perjuicio del principio de libertad probatoria que rige en la mayoría de las legislaciones de forma de nuestro país, esas herramientas deberían ser introducidas en ellas para equilibrar la persecución penal del Estado con los derechos fundamentales de los investigados. Esta reflexión es parte de una discusión que debate acerca de la necesidad —o no— de incorporar a los códigos procesales nuevas medidas de investigación adaptadas a las tendencias digitales.

El desafío de las *deepfakes*

Los perpetradores se están volviendo cada vez más sofisticados y utilizan tecnología de última generación. Así, elaboran *deepfakes*: imágenes hiperrealistas manipuladas y modificadas de manera digital, que muestran a niños, niñas, adolescentes y adultos haciendo o diciendo cosas que nunca sucedieron en realidad, muchas veces en situaciones sexuales.

Las *deepfakes* no se encuentran legisladas en algunos países de la región, lo que convierte en un gran desafío internacional la investigación y el procesamiento de casos de abuso sexual en línea, sobre todo cuando se trata de este tipo de imágenes.

Segunda parte

Cómo proceder ante delitos en entornos digitales que afectan a NNyA

En las páginas que siguen se desarrollará una guía completa e indicativa de los pasos a seguir cuando se investiguen *grooming* y delitos de explotación sexual de NNyA cometidos en entornos digitales, junto con sus derivaciones. Entre otros aspectos, se abordará cómo realizar la trazabilidad completa y el tratamiento de la evidencia digital.

Vale destacar que muchas veces no se puede separar una conducta delictiva de la otra, porque cuando se investigan casos de explotación sexual de NNyA es común que al analizar los dispositivos de almacenamiento informático se hallen conversaciones entre el *groomer* y la/s víctima/s. De la misma manera, a raíz de denuncias de *grooming*, y al investigar el campo informático, es factible detectar que el autor difundió en una red internacional de explotación sexual de NNyA las imágenes o videos obtenidos o recibidos del niño, niña o adolescente que estaba acosando. Además, es común que, en uno u otro caso, se derive en una situación de abuso sexual interfamiliar o dentro de un círculo íntimo (escuelas, gimnasios, clubes, etc.).

En este sentido, y partiendo de la base de un sistema procesal penal moderno, como es el acusatorio ya instalado en muchos países de la región y en la mayoría de las provincias argentinas, la investigación del caso se encuentra en cabeza del fiscal, quien fija una hipótesis o línea de investigación, cuya estrategia es discutida con las fuerzas especializadas, tendientes a corroborar la comisión del hecho e identificar al autor o los autores que en él intervinieron.

Al recibir los casos, es fundamental que la fiscalía haga una proyección de la investigación de cara al juicio oral. Es decir, que elabore su propia teoría del caso o hipótesis de investigación, con sus

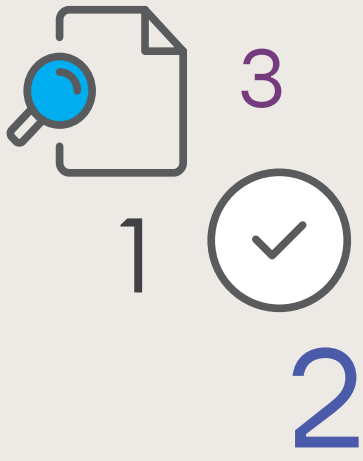
fortalezas y debilidades, en concordancia con el área informática. Para que las investigaciones en entornos digitales tengan éxito, el binomio jurídico-técnico debe atravesar el caso desde el principio hasta su fin. Por su parte, la defensa hará idéntico trabajo de acuerdo a su propia teoría del caso.

Para que las investigaciones en entornos digitales tengan éxito, el binomio jurídico-técnico debe atravesar el caso desde el principio hasta su fin.

Los jueces también

Es muy importante comprender que si bien todas las provincias implementaron un sistema acusatorio, ello no implica que solo el fiscal deba obtener las capacidades para investigar, sino también los jueces. Para realizar un debido control del procedimiento y velar por las garantías constitucionales, los jueces deben adquirir estas destrezas, pues ello les permitirá discernir si la actividad procesal, el tratamiento de la evidencia digital y su trazabilidad, presentados por el fiscal en el juicio, son correctos y, en consecuencia, tomar decisiones de alta calidad.

Tres pasos fundamentales para una investigación eficiente



Para poder llevar adelante una investigación eficiente de delitos contra NNyA en entornos digitales se necesita cumplir con tres pasos fundamentales. Estos tienen por objetivo identificar al usuario investigado y corroborar la hipótesis del fiscal.

1. Identificar y determinar el hecho a investigar de acuerdo a una figura legal. De esto dependerán las medidas de prueba que podrán solicitarse.
2. Resguardar la evidencia digital. Por su volatilidad, esta se puede perder rápidamente.
3. Tomar diferentes medidas para identificar e investigar al usuario sospechoso: requerimientos a ISP, tareas de constatación, orden de presentación, allanamiento, análisis de fuentes abiertas: *big data*, inteligencia artificial (IA), internet de las cosas (IoT).

Paso 1. Identificar y determinar el hecho a investigar subsumible en una figura legal

El primer paso consiste en delinear la teoría del caso: identificar los hechos motivo de la denuncia recibida, adaptarlos a un tipo penal y elaborar, en consecuencia, una estrategia de investigación basada en la producción de diferentes medidas de prueba. Esta tarea es del fiscal, quien procederá a la investigación.

Vale aclarar que existen diferentes formas en que los casos de explotación sexual de NNyA ingresan a la Justicia argentina, que se presentan a continuación:

National Center for Missing and Explotation Children (NCMEC). A fines de 2013, la Fiscalía General de CABA firmó un convenio con el NCMEC[10] que permite que el Ministerio Público Fiscal de CABA reciba todos los reportes de actividades sospechosas que se detecten de usuarios de internet en nuestro país.

En Estados Unidos existe una obligación legal específica para los proveedores de servicios electrónicos respecto de la notificación de material de abuso sexual de NNyA (CSAM). Conforme a la normativa **18 USC § 2258A**, los proveedores deben **reportar al NCMEC** cualquier caso de CSAM del que obtengan **conocimiento efectivo**, "tan pronto como sea razonablemente posible", bajo sanciones pecuniarias en caso de incumplimiento. Esta obligación **no se extiende a otros tipos de contenido ilegal**, ya que la ley no impone a los proveedores el deber de reportar ni monitorear de forma general cualquier contenido ilícito presente en sus redes.

Ahora bien, el Ministerio Público Fiscal de CABA es el encargado de seleccionar los casos a investigar. Una vez establecido desde qué provincia se conectó el eventual delincuente para cometer el delito, se lo envía, a través de una VPN[11], para asegurar el anonimato, a la autoridad fiscal de investigación de esa provincia.

Operaciones internacionales. Es habitual que cuando en algún país se está investigando una red de explotación sexual de NNyA y se detecta que desde la Argentina se habría distribuido, facilitado, publicado o producido material de abuso sexual de NNyA, se reporte la *noticia criminis*, a través de Interpol, a la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas de la Ciudad Autónoma de Buenos Aires (UFEDyCI), que la canaliza en la División Delitos Cibernéticos contra la Niñez y Adolescencia de la Policía Federal Argentina.

También, la Oficina de Investigaciones de Seguridad Nacional de los Estados Unidos (HSI, por sus siglas en inglés)[12] lleva a cabo investigaciones en otros países y reporta a la Argentina cuando detecta que, a través de redes para compartir P2P, usuarios nacionales facilitan videos de NNyA en actividades sexuales o exhibiendo sus partes genitales con fines predominantemente sexuales.

Por otro lado, una de las últimas modalidades consiste en facilitar, intercambiar y vender videos y fotografías de NNyA siendo abusados sexualmente por adultos a través de grupos de Telegram, WhatsApp y Signal, pues la encriptación de mensajes dificulta al investigador identificar a los autores. Esos casos suelen llegar a la Argentina a través de actuaciones de las fuerzas internacionales de la ley.

10. Resolución FG. 435/2013 del 12 de noviembre de 2013.
11. *Virtual private network*: red privada virtual que permite ocultar o modificar la ubicación y la dirección IP del usuario.
12. Se especializa en delitos transnacionales, entre ellos, la explotación sexual de NNyA. Es la principal rama investigativa del Departamento de Seguridad Nacional (DHS) de EE. UU., una agencia federal que combate el crimen transnacional.

Es importante conocer cómo funciona una red P2P para luego armar la estrategia de investigación tendiente a determinar qué autores compartieron o facilitaron los videos sexuales de NNyA y cómo desarrollaron dicha actividad ilícita.

Respecto a los casos de *grooming*, estos ingresan en su mayoría a través de denuncias realizadas por los padres de los NNyA acosados sexual y virtualmente. En general, estas denuncias derivan en otras líneas de investigación con nuevos damnificados, cuyos progenitores, en gran parte de los casos, no tienen conocimiento de que sus hijos han sido víctimas de esta conducta.

No obstante, también es común que, del análisis de los dispositivos informáticos secuestrados en casos de explotación sexual de NNyA, se hallen conversaciones e intercambios de fotos sexuales entre adultos y NNyA. Generalmente las denuncias se realizan ante los Ministerios Públicos Fiscales, ante alguna de las fuerzas policiales especializadas o a través de los canales de denuncia previstos por diferentes ONG que tratan la problemática, las que incluso alientan que los propios NNyA informen a sus padres y docentes sobre este tipo de abuso, para la realización de la correspondiente denuncia.

Paso 2. Resguardar y preservar la evidencia digital

A partir de la denuncia recibida, o tomando conocimiento de un incidente de tráfico de material de explotación sexual de NNyA, existen **dos líneas de investigación** posibles por parte de los fiscales, y con la colaboración de la policía especializada, en las que la extracción y el resguardo de la evidencia digital son centrales.

Información con la que cuenta la víctima (casos de *grooming*). En general, la víctima posee la información necesaria para los investigadores cuando advierte que fue acosada y desea denunciar, ya sea a través de sus progenitores o algún familiar. Se trata de *chats*, mensajes, *mails*, fotografías o videos recibidos, etc. que están en sus dispositivos de almacenamiento informático y que pone a disposición de los investigadores para su correcta preservación. También comprende registros de acceso en sus sistemas en relación a algún ataque.

Es importante que, para la correcta preservación de la información, los denunciantes la aporten inmediatamente, de manera intacta y sin borrarla total o parcialmente, ya que su recuperación se torna dificultosa.

Información a requerir respecto del usuario investigado (casos de *grooming* y de explotación sexual de NNyA). Esta línea de investigación es utilizada, en los casos de explotación sexual de NNyA, cuando se reciben los reportes de NCMEC en los cuales aún no hay víctimas identificadas, pero a partir de la información se focaliza la investigación hacia el o los sospechosos. También, cuando en los casos de *grooming*, y a raíz de la información entregada previamente por la víctima,

se identifican los datos que permiten dar con el usuario que posiblemente sea el autor del hecho (ver en detalle en el paso 3).

Para ello se deben identificar los datos necesarios para requerir información a las distintas empresas respecto del usuario. Se deben utilizar las herramientas para preservar la información que brindó la víctima sobre el usuario investigado hasta tanto sea aportado por la ISP.

El término *preservar* es definido por el Diccionario de la Real Academia Española como: proteger, resguardar anticipadamente de alguien o algo de un eventual daño o peligro. Ello implica que, al definir ciertas técnicas o mecanismos para la preservación de la evidencia digital, se está previendo que existe la posibilidad de un daño o peligro (Di Iorio, 2016). Por esa razón, se debe asegurar la evidencia de forma tal que pueda demostrarse su trazabilidad a lo largo de todo el proceso, con la debida cadena de custodia digital que debe comenzar.

UFED: herramienta forense para extraer la información

La herramienta forense utilizada para extraer la información almacenada en dispositivos móviles es el Universal Forensic Extraction Device (UFED)[13]. Entre otras cosas, permite obtener el listado de contactos, datos acerca del dispositivo analizado, recuperar historial de conversaciones a través de plataformas de mensajería instantánea como WhatsApp, recuperar imágenes y videos almacenados e incluso, en algunos casos, también archivos que fueron borrados.

A partir de esta extracción se obtiene un informe técnico en formato digital, que detalladamente ordena la información extraída, catalogándola por tipo de aplicación y de documento, permitiendo incluso filtrar la información mediante búsquedas específicas. Este punto no es menor, ya que la cantidad de información que suele hallarse en los dispositivos telefónicos es muchísima, por lo que esto facilita la búsqueda cuando es preciso hallar, por ejemplo, una conversación determinada entre el *groomer* y el niño, niña o adolescente víctima.

La preservación la ordena el fiscal a la policía especializada, pues esta posee las herramientas adecuadas para efectuarla. El rol del juez en esta instancia es corroborar, *a posteriori*, que no se haya alterado la evidencia, y para ello debe conocer cómo se realiza la preservación y para qué sirve en el marco de una investigación. Para la preservación de los datos acopiados en los dispositivos de almacenamiento informático no es necesaria una autorización judicial previa, pues se trata de un clonado, un aseguramiento, una copia de datos; no se analiza ni se pericia.

13. Es una herramienta forense utilizada para la extracción y el análisis forense de los datos insertos en los móviles: registros de llamadas, incluso historiales de llamadas borrados de la tarjeta SIM, contactos, datos del teléfono (IMEI/ESN, número de teléfono), ICCID e IMSI, fotografías, videos, archivos de sonido, información de localización de la SIM: TMSI, MCC, MNC, LAC y geoetiquetas gráficas en Google Maps.

Figura 2. Extracción de información mediante UFED

Fuente: Elaboración propia.

Alternativas al UFED

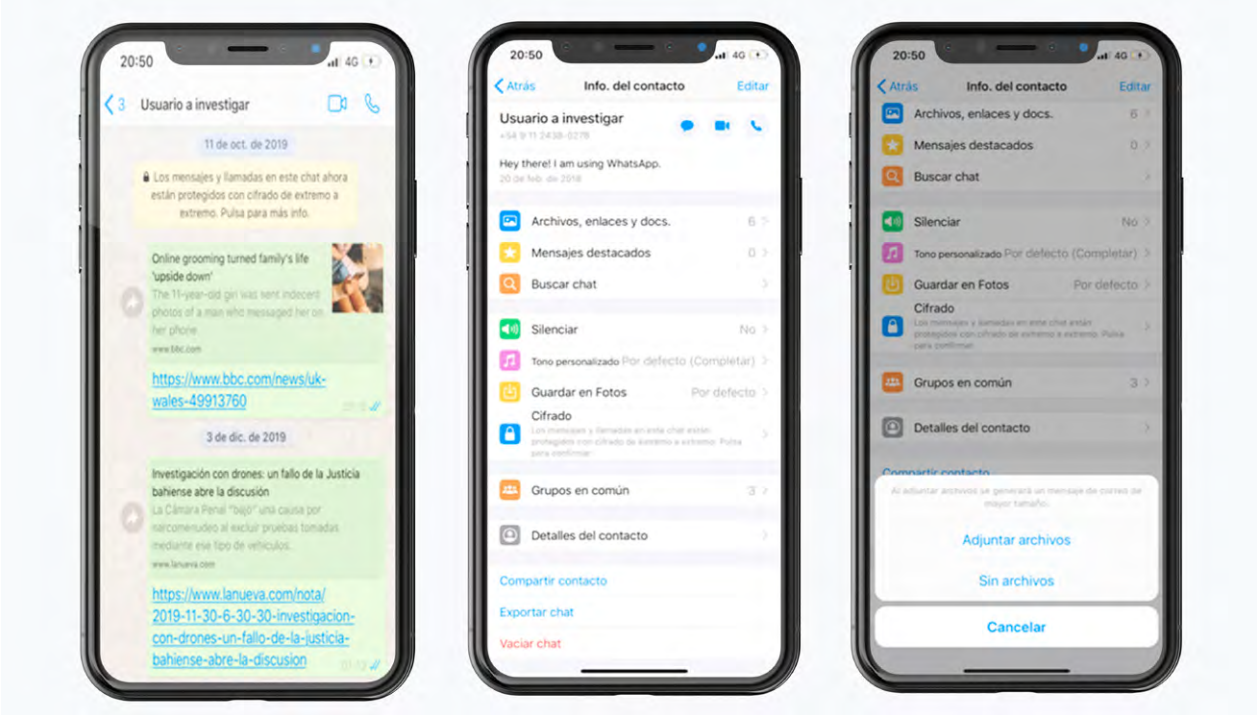
Tanto cuando la víctima aporta su celular como cuando se logra secuestrar el celular del posible autor y, para el caso de que no se posea una herramienta forense como el UFED, o bien sus credenciales no estén debidamente actualizadas, se deberán adoptar otras alternativas para preservar la evidencia digital y evitar su pérdida, ya sea por un posterior borrado o por el extravío del dispositivo de almacenamiento.

El fiscal o el personal policial especializados son quienes realizan esta acción, que será explicada al juez con posterioridad para demostrar la legítima trazabilidad.

A continuación se presenta cómo se realiza, dependiendo de la red social o la plataforma de mensajería. También se pueden obtener los registros de llamadas y de correos electrónicos.

WhatsApp

Una forma rápida y segura de resguardar mensajes, fotografías o videos recibidos a través de la plataforma WhatsApp es exportando en simples pasos el chat a preservar y enviarlo a una cuenta de correo oficial para su posterior resguardo, dejando constancia de todo lo actuado. Al momento de efectuar la extracción, la plataforma preguntará si se realiza con o sin los archivos adjuntos con los que cuente ese chat. Es recomendable conservar los archivos ya que, si en el marco de las conversaciones que se pretende resguardar hubo intercambio de imágenes y videos —y no fueron borrados—, también se estarán preservando. El sistema crea un archivo comprimido que contendrá, por un lado, un archivo en formato .txt con toda la conversación —contenido, interlocutores, fecha y hora de mensajes— y, de forma separada, los archivos correspondientes a esa conversación (Dupuy, 2022).



Si bien en el ejemplo gráfico la exportación del chat fue realizada a través de un teléfono Apple, los dispositivos con sistema operativo Android también tienen esta opción.

Redes sociales

De forma similar se puede preservar todo el contenido de las cuentas de redes sociales de una víctima.

En el caso de Instagram se debe contar con los datos de acceso a la cuenta. Se debe ingresar a:

"Configuración" / "Privacidad y seguridad" / "Descargar datos"

Allí aparecerá la opción de obtener una copia de todo lo que ese usuario compartió en Instagram —fotos, comentarios, información de perfil, entre otros—, lo cual será enviado mediante correo electrónico. La propia firma informa que podrá demorar hasta 48 horas en remitir dicha información (Dupuy, 2022).

Meta, por su parte, prevé un sistema mucho más detallado para resguardar información del propio usuario. Se debe ingresar a:

"Configuración y Privacidad" / "Tu información en Facebook" / "Acceder a tu información", y presionar allí la opción "Descargar tu información"

En esta instancia, permitirá solicitar una copia de la información que se seleccione —publicaciones, fotos y videos, comentarios, mensajes, historias, etc. —, pudiendo también elegir que se descargue la totalidad de la información.

También posibilitará seleccionar el período de tiempo respecto del cual se quiere hacer la descarga. Al finalizar la selección, y luego de presionar "Generar archivo", se obtendrá un archivo comprimido con la descarga seleccionada, lo que será informado en la solapa de notificaciones del usuario una vez que esté completa la descarga.

Registro de llamadas

El resguardo del registro de llamadas también es una prueba relevante para los casos de *grooming*, ya que puede ocurrir que el *groomer* se comunique con su víctima telefónicamente o a través de WhatsApp.

Es posible y aconsejable resguardar este tipo de información también mediante la utilización del UFED. Si no se cuenta con esta herramienta se podrá hacer de forma manual, y será suficiente para acreditar la existencia de ese registro.

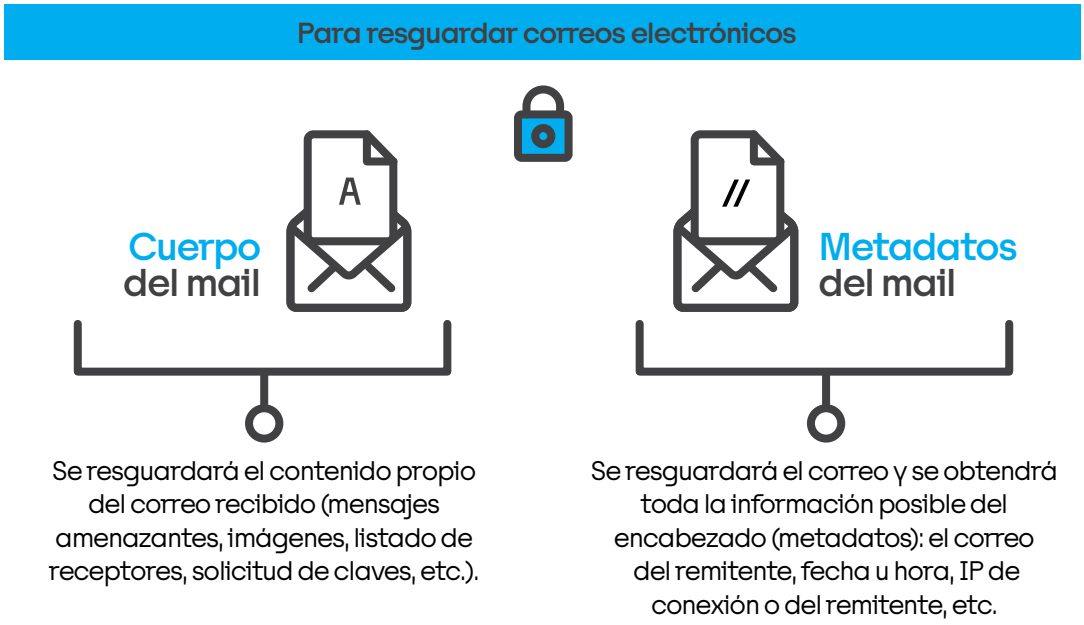
Desde el teléfono de la víctima, se procederá de la siguiente forma:

1. Ingresar al listado de llamadas entrantes y salientes.
2. Obtener una captura de pantalla de ese listado.
3. Labrar la constancia pertinente.
4. Solicitar a la empresa telefónica correspondiente el registro de llamadas entrantes y salientes del abonado telefónico para corroborar dicha circunstancia.
5. Identificar al abonado telefónico con el que se estuvo comunicando la víctima.

Resguardo de correos electrónicos

Para el caso de que la conducta se haya llevado a cabo mediante la utilización de correos electrónicos, es importante que, al momento de preservarlos, se conserve el correo desde el cual fueron enviados, el contenido del mensaje y sus metadatos.

Figura 3. Resguardo de correos electrónicos



Fuente: Elaboración propia.

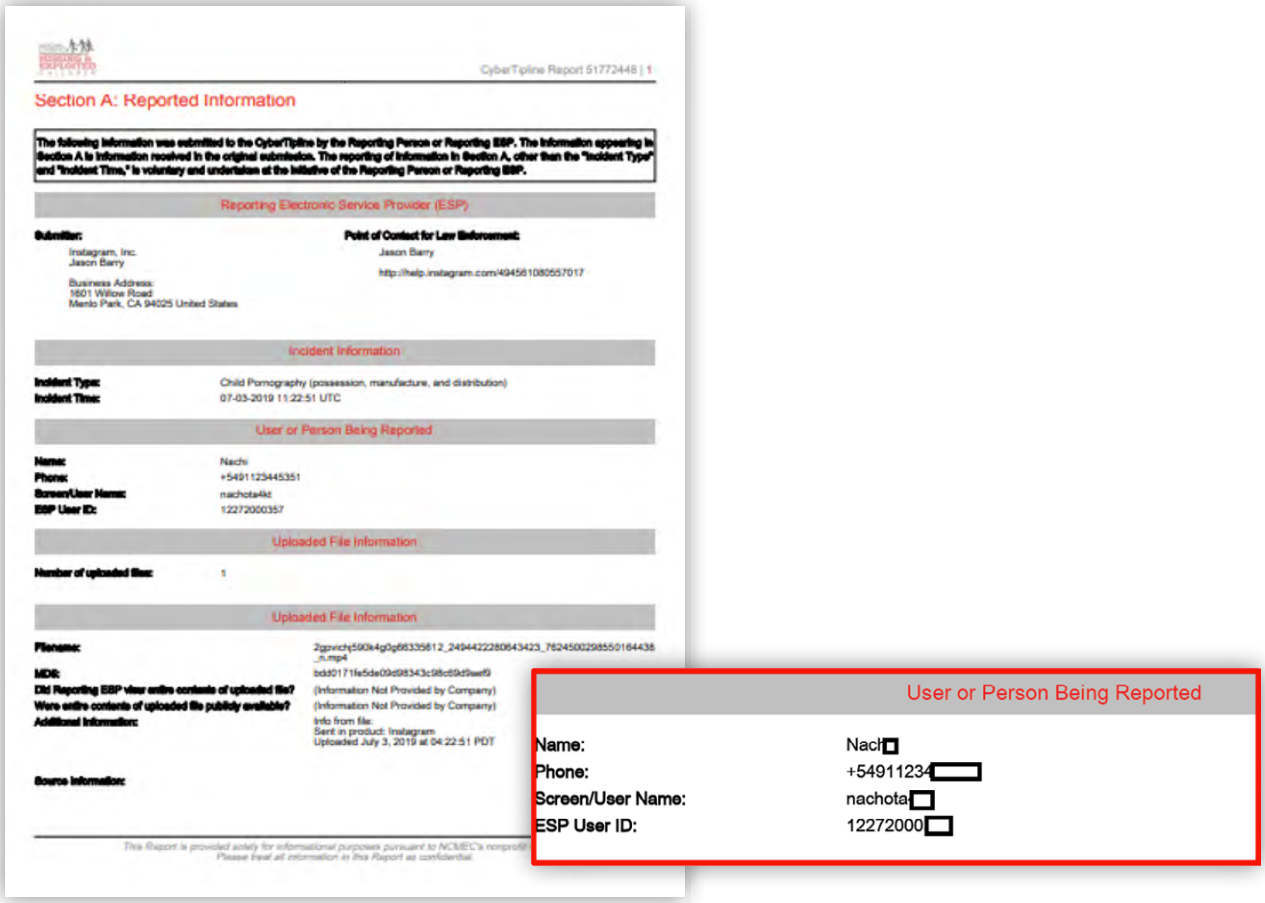
Información de discos rígidos

Como se explicó, cuando la evidencia se encuentre en un teléfono celular, la extracción de la información se lleva a cabo mediante herramientas específicas, como el UFED. En cambio, cuando la información está almacenada en discos rígidos —computadoras, pendrives, etc.—, de acuerdo a las buenas prácticas de informática forense, la extracción se inicia a través de la obtención de una imagen forense, que constituye una réplica exacta del contenido del soporte de almacenamiento, una copia idéntica de todos y cada uno de los *bits* contenidos en él, lo que incluye la totalidad de los archivos almacenados, el espacio libre y no asignado, el "*Master File Table*" en el orden preciso que se encuentran en el original.

Paso 3. Identificar al sospechoso e investigar la maniobra delictiva

Cuando se trate de un caso iniciado a partir de un incidente reportado por el NCMEC, el usuario a investigar ya estará determinado. Ello es parte de la investigación que realiza el fiscal o bien el policía especializado con orden del fiscal.

A continuación, se presenta un ejemplo en el que el usuario es de la red social Instagram.



CyberTipline Report 51772448 | 1

Section A: Reported Information

The following information was submitted to the CyberTipline by the Reporting Person or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:
Instagram, Inc.
Jason Barry

Business Address:
1601 Willow Road
Menlo Park, CA 94025 United States

Point of Contact for Law Enforcement:
Jason Barry
http://help.instagram.com/494561080557017

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-03-2019 11:22:51 UTC

User or Person Being Reported

Name: Nachi
Phone: +5491123445351
Screen/User Name: nachota4kt
ESP User ID: 12272000357

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: 2gpvichj590k4g0g86335612_2494422280643423_7624500298550164438_n.mp4
MD5: bdd01711e5de09d98343c98c89d9eef9
Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)
Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
Additional Information: Info from file:
Sent in product: Instagram
Uploaded July 3, 2019 at 04:22:51 PDT

Source Information:

This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit
Please treat all information in this Report as confidential.

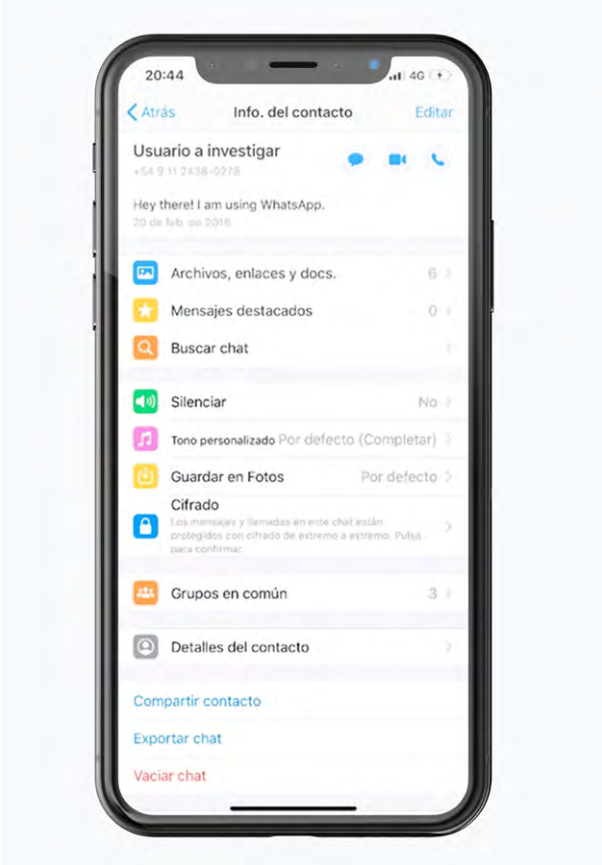
User or Person Being Reported

Name: Nach
Phone: +54911234
Screen/User Name: nachota
ESP User ID: 12272000

En cambio, para los casos que se inicien a raíz de una denuncia particular, y luego de resguardada la evidencia aportada por la víctima, el paso siguiente es identificar al usuario a investigar, cuya información luego se requerirá a las empresas prestatarias de servicio pertinentes, como se verá más adelante. Para ello, es importante preservar el usuario a investigar, para luego requerir correctamente la información de acuerdo a la red social o plataforma utilizada por el autor para cometer el delito (Dupuy, 2022).

WhatsApp

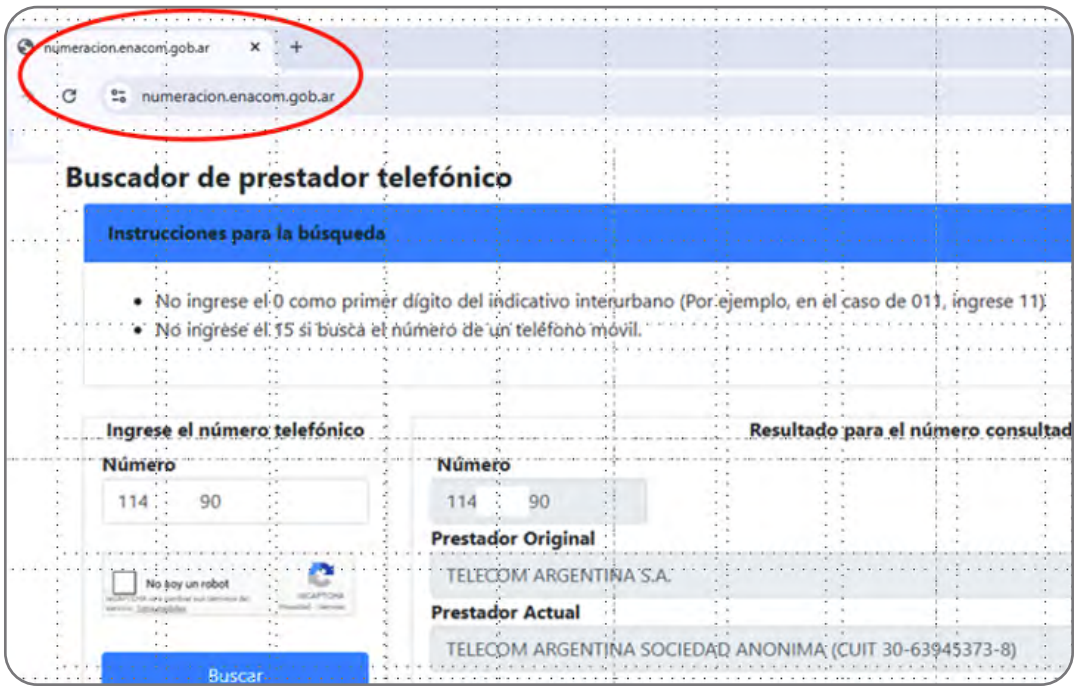
En aquellos casos en los que el autor se haya contactado con su víctima a través de esta plataforma, o que se haya facilitado material de explotación sexual de NNyA, para identificar al usuario a investigar es necesario contar con el número de abonado telefónico que envió esos mensajes —prefijo, código de área y número telefónico—, cuyos datos luego serán requeridos a la empresa de telefonía pertinente.



Los datos solicitados por el fiscal directamente a la empresa telefónica serán:

- **Titularidad de ese abonado (nombre, apellido, DNI).**
- **Tipo de servicio (prepago o factura).**
- **Domicilio.**
- **Fecha de alta de servicio.**

En la Argentina, a fin de determinar a qué empresa corresponde un abonado telefónico, se puede consultar el sitio **numeracion.enacom.gob.ar**.



Redes sociales

La forma de identificar al usuario a investigar dependerá de la red social que se haya utilizado. El punto en común a destacar de todas ellas es que el nombre de usuario, nombre visible o *vanity name* de la cuenta a investigar no siempre será o coincidirá con el ID que se necesita para su correcta identificación y posterior solicitud a las ISP. Puede suceder que el *vanity name* coincida entre muchos usuarios, pero no así el ID de cada uno de ellos. Es importante poder identificarlo, ya que un usuario podrá cambiar su nombre visible, pero jamás podrá modificar el ID que lo identifica.

La información de suscripción del usuario que se solicitará a las empresas será la siguiente:

- **Nombre.**
- **Fecha de nacimiento.**
- **Fecha de creación de la cuenta.**
- **IP de creación.**
- ***Logs* de conexión.**
- **En última instancia, información de contenido (texto y adjuntos de un correo electrónico, mensajes y adjuntos intercambiados en redes sociales, etc.).**

Facebook exige que, al momento de solicitarle información respecto de un usuario, se le informe el ID o la URL que lo identifica. Este se puede hallar visitando el perfil de dicho usuario, en la barra del buscador, luego de **www.facebook.com/**. La información que se encuentra inmediatamente después de esa barra será la necesaria al momento de efectuar una solicitud de información.

Lo mismo ocurrirá con el resto de las redes sociales, como **Instagram** o **Snapchat**.

Daño inminente

Cuando se trata de casos de emergencia en los que es urgente la obtención de información, las ISP tienen previstos canales para saltear algunos de los pasos previamente explicados.

Estos canales pueden ser utilizados en casos de:

- Daño inminente a un NNyA.
- Riesgo de muerte o lesiones físicas graves a cualquier persona.

Al momento de realizar la solicitud:

- La deben presentar las fuerzas de la ley (MPF, juez, policía).
- Hay que especificar en el asunto que se trata de una emergencia.
- Utilizar plataformas de internet especialmente previstas por las ISP.
- Identificar al usuario cuya información se solicita (nombre de usuario, URL, ID).
- Identificar a la persona que se encuentra en riesgo de muerte o de lesión física grave.
- Justificar la naturaleza de la emergencia.
- Especificar qué tipo de información se requiere y por qué es relevante para evitar la emergencia.
- Adjuntar capturas o cualquier evidencia que pueda resultar de interés.
- Algunas ISP piden firma del solicitante.

Conservación rápida de datos

Uno de los enemigos de las investigaciones en entornos digitales es el tiempo. Entre que se detecta la comisión del delito en el ciberespacio y se requiere información a las ISP en el marco de una investigación, suele pasar un tiempo considerable en el que puede ocurrir que las empresas borren la información de los usuarios por cuestiones de política empresarial; esto se debe a que no en todas las legislaciones está obligada su conservación por un tiempo determinado.

Es decir, dada la naturaleza volátil y perecedera de las pruebas digitales, los investigadores deben asegurarse que los protocolos de conservación de datos se activen rápidamente. Sin embargo, la conservación debe distinguirse del acceso. No permite que se supriman o alteren datos, pero no autoriza su recuperación o revisión[14].

Es importante señalar que en la Argentina no existe regulación alguna al respecto.

En consecuencia, se debe solicitar a las empresas su conservación, es decir, que omitan suprimir la información respecto de un usuario con el fin de evitar que las evidencias se pierdan antes de que sean incorporadas en el marco de la investigación.

No es una medida probatoria, pues no se obtiene prueba, simplemente es una solicitud de *"quick freeze"* —que conserven toda la información del usuario a ese momento— a las diferentes empresas para que aseguren los datos respecto de un usuario determinado.

La conservación rápida de datos exige que se efectúe en el marco de una investigación penal en curso y respecto de datos que ya se encuentran almacenados en algún soporte electrónico o digital, pudiendo tratarse tanto de datos de tráfico como de contenido. En ese sentido, el art. 16 del Convenio de Budapest, al cual nuestro país ha suscripto, se refiere a la conservación rápida de datos informáticos almacenados en los casos en los que "los datos informáticos resultan especialmente susceptibles de pérdida o de modificación".

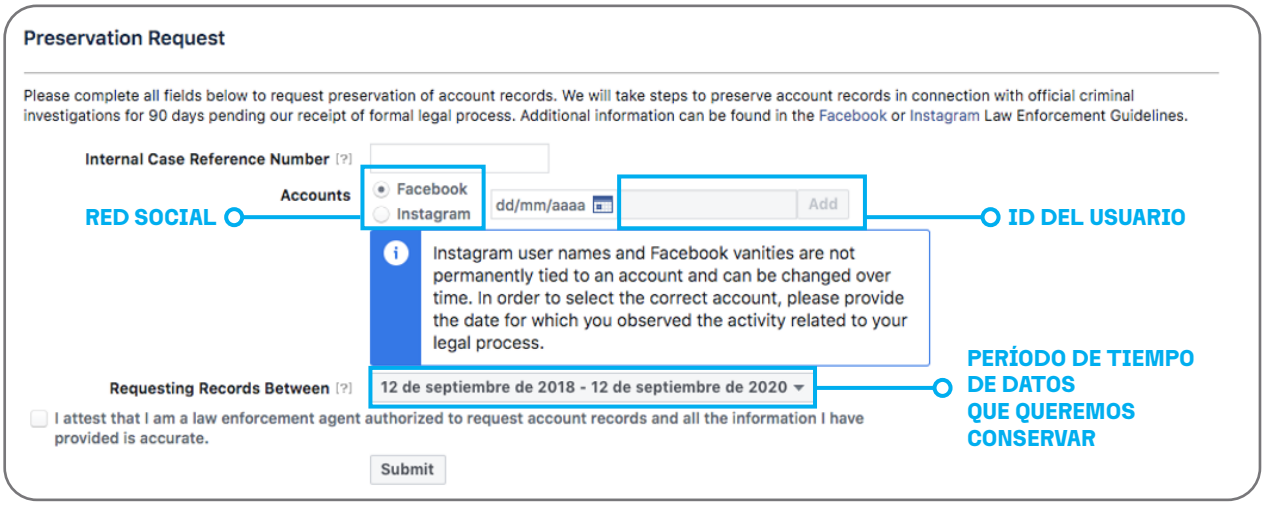
Cómo realizar un pedido de conservación

Para realizar un pedido de conservación en relación a un usuario de Facebook o Instagram, al ser Instagram un servicio de Facebook, el portal habilitado para las fuerzas de la ley es el mismo: **https://www.facebook.com/records/**

En ambos casos, tanto las fuerzas policiales como funcionarios del Ministerio Público Fiscal o del Poder Judicial podrán efectuar el pedido de conservación, el cual se realiza directamente desde la plataforma habilitada específicamente para investigadores oficiales y fuerzas de la ley, sin necesidad de confeccionar ningún oficio, y sin orden del juez, toda vez que no se están requiriendo datos, sino que la empresa NO los borre.

14. Para más información, ver las Directrices para fiscales sobre la recopilación de las pruebas digitales de la UNESCO y la International Association of Prosecutors (pág.10 y ss.).

En el marco de dicha conservación, y dependiendo de si se trata de un usuario de Facebook o de Instagram, se inserta el ID identificado y el período de tiempo de la actividad del usuario que se quiere preservar. Esta información será conservada por el término de 90 días, plazo que podrá ser prorrogado por otros 90 días.



Fuente: https://www.facebook.com/records

Así como se ha detallado el proceso establecido por Facebook para conservar datos de los usuarios de sus redes, cada plataforma o red social ha establecido su propio mecanismo, los que se deben conocer a fin de poder efectuar una correcta conservación rápida de datos.

Tabla 1. Plataformas a través de las cuales se efectúan peticiones

Plataformas	Preservación de la cuenta
https://lers.google.com/	Sin oficio
https://www.facebook.com/records/	Sin oficio
https://www.facebook.com/records/	Sin oficio
https://www.whatsapp.com/records/	Sin oficio
https://leportal.microsoft.com/home	Sin oficio
https://legalrequests.twitter.com	Sin oficio
https://leportal.microsoft.com/home	Sin oficio
https://safety-enforcement.tiktok.com/	Con oficio
https://less.snapchat.com/?lang=ex-ES	Con oficio
https://app.kodexglobal.com/	Con oficio

Fuente: Elaboración propia.

Solicitud de la información (datos de tráfico) respecto del usuario identificado como sospechoso

El mecanismo habitual para pedir datos de usuario que se encuentran en otra jurisdicción es a través de rogatorias internacionales o mediante la utilización de tratados de cooperación internacional de asistencia mutua en asuntos penales[15].

Sin embargo, dada la naturaleza de las investigaciones en entornos digitales o que involucran evidencia digital, es fundamental recibir los datos del usuario en el menor tiempo posible y antes de que se pierdan o sean borrados.

Por ello, y en razón de la volatilidad de la evidencia digital y de lo engorroso y burocrático que representa la solicitud de la información a través de los tratados tradicionales internacionales, se ha generado en la práctica una costumbre de intercambio informal de datos a través de los correspondientes portales de cada una de las empresas habilitados para las fuerzas de la ley (Dupuy y Kiefer, 2020).

Debido a que la colaboración es voluntaria, los requisitos para solicitar información a las empresas internacionales varían según sus políticas internas. En ese sentido, a continuación se compartirán los aspectos formales que exige cada empresa para brindar información a través de los mencionados canales informales.

Google

Administra servicios tales como Gmail, Google Drive, Google Hangouts, Google Photos, etc. Para solicitar datos de registración de un usuario y logueos, requiere, en primer lugar, la existencia de una cuenta de correo investigada.

Habiendo identificado dicha cuenta, se deberá librar un oficio vía correo electrónico a la casilla prevista por la firma para estos pedidos. Este correo debe incluir:

- Encabezado: CUSTODIANS OF RECORDS GOOGLE INC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, Estados Unidos de América.
- Firma del juez interviniente.
- Datos del usuario investigado y tipo de información requerida: datos de creación de cuenta, *logs* de conexión, registro transaccional, cuentas de correo o abonados telefónicos asociados, etc[16].

Facebook

Administra los servicios de Instagram y WhatsApp, entre otros, con sus propios requisitos. Ha creado portales *online* específicos para que los operadores judiciales y las fuerzas policiales diligencien estas requisitorias.

15. Por ejemplo, la Convención Interamericana sobre Asistencia Mutua en Materia Penal. Además, la Argentina ha suscripto con EE. UU. —país donde se encuentran alojadas la mayoría de las empresas cuya información se necesita en investigaciones de este tipo— el Tratado de Asistencia Jurídica Mutua en Asuntos Penales, Ley 24.034 (sancionada el 27 de noviembre de 1991), donde también se establece el mecanismo de cooperación para requerir información o documentación en el marco de investigaciones penales de un Estado al otro. Sin embargo, en la práctica, este medio para solicitar información no resulta idóneo, ya que el procedimiento tiene formalidades y es largo, y pueden transcurrir meses hasta que se recibe la información requerida.
16. Para mayor información acerca de las políticas de Google en relación a peticiones internacionales de información, visitar: https://support.google.com/transparencyreport/answer/9713961?hl=en

Para el caso de usuarios de Facebook e Instagram el portal es **https://www.facebook.com/records**, y para solicitar la información se debe presentar un oficio firmado por el juez interviniente.

Microsoft

Exige que la requisitoria se remita vía mail y que esté firmada por el juez o fiscal, indistintamente.

Skype

Requiere que el oficio con la solicitud sea remitido en inglés[17].

X

No ha habilitado el canal informal para brindar información en el marco de este tipo de investigaciones, salvo casos extremos, requiriendo que se utilicen los canales formales, es decir, el Tratado de Asistencia Jurídica Mutua en Asuntos Penales firmando con EE. UU.[18].

Tipos de datos en el Convenio sobre la Ciberdelincuencia

Datos relativos al tráfico (art. 1 d). Son los datos generados por sistemas informáticos para encaminar una comunicación. Incluyen:

- Origen (número telefónico, IP u otro identificador).
- Destino.
- Ruta.
- Fecha y hora (GMT).
- Tamaño.
- Duración.
- Tipo de servicio subyacente (e-mail, transferencia de archivos, mensajería instantánea).

Son datos auxiliares, pueden tener duración efímera y su conservación rápida es clave. No siempre todas las categorías están disponibles ni son necesarias para cada investigación.

Datos de contenido. Corresponden al mensaje o información transmitida:

- Texto de un chat.
- Cuerpo de un e-mail.

17. Para mayor ilustración acerca de las políticas y requisitos exigidos por Microsoft y Skype, visitar: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.
18. Para conocer en mayor detalle las normas operativas y requisitos exigidos por la firma X para las fuerzas de la ley que solicitan información, visitar: https://help.twitter.com/es/rules-and-policies/twitter-law-enforcement-support y https://legalrequests.twitter.com/forms/records.

Son los que mayor protección requieren por su impacto en la intimidad y la privacidad.

Datos relativos a los abonados (art. 18.3). Información que poseen los proveedores sobre sus usuarios, distinta de tráfico y contenido. Incluye:

- Identidad del abonado.
- Domicilio de facturación o instalación.
- Tipo y período del servicio.
- Número telefónico.
- Datos de facturación y pago.

En la Tabla 2 se observan los requisitos formales exigidos por cada ISP, diferenciando si se trata de datos de tráfico o de contenido. En todos los casos, teniendo en cuenta la implicancia de solicitar datos de tráfico, es el juez, a pedido del fiscal, quien debe requerirlos con la modalidad señalada más arriba.

Tabla 2. Requisitos para solicitar información

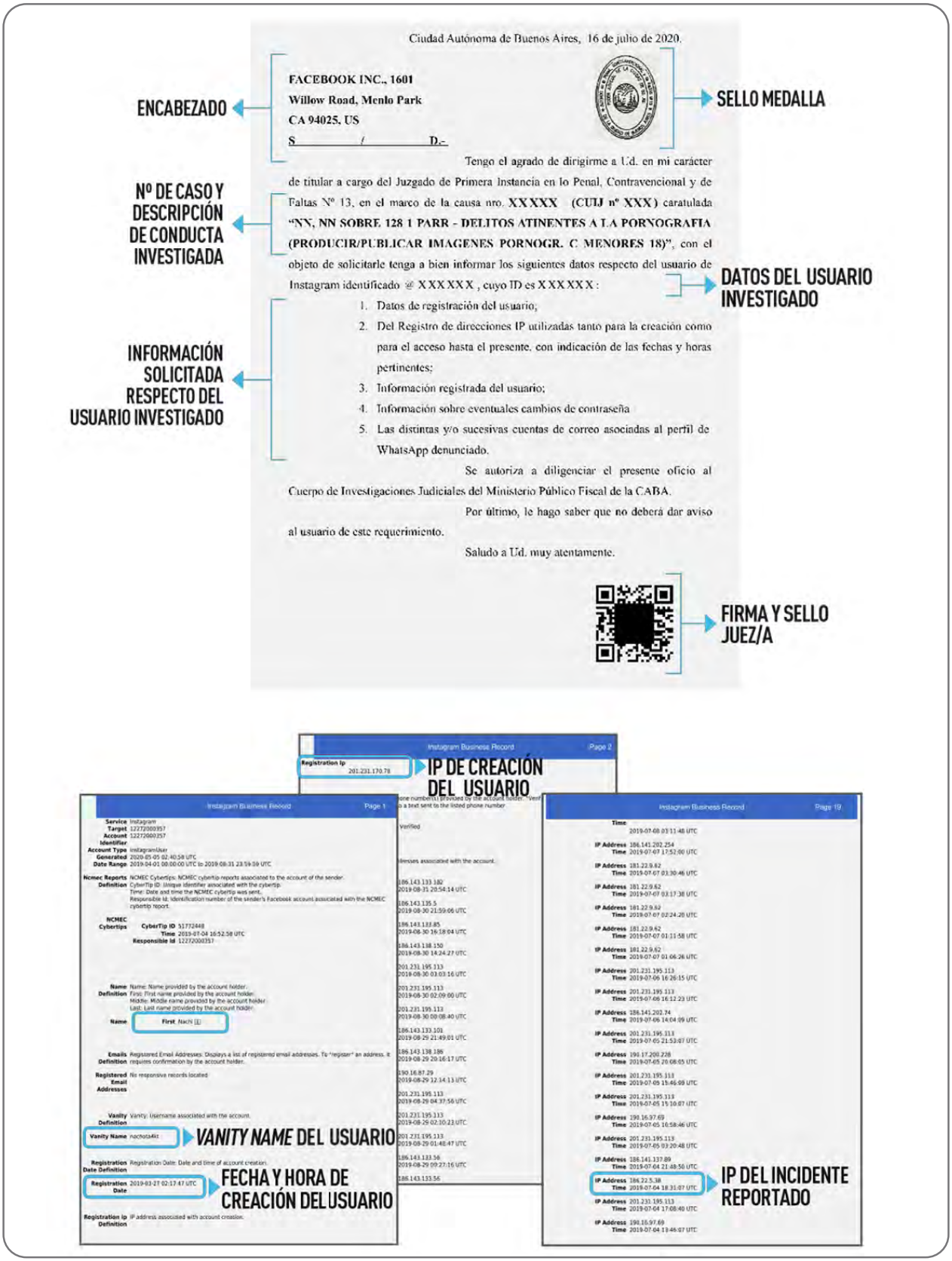
Plataformas a través de las cuales se efectúan peticiones	Datos de registración y conexión	Datos de contenido
https://lers.google.com/	Oficio firmado por juez *	MLAT
https://www.facebook.com/records/	Oficio firmado por juez *	MLAT
https://www.facebook.com/records/	Oficio firmado por juez *	MLAT
https://www.whatsapp.com/records/	Oficio firmado por juez *	MLAT
https://leportal.microsoft.com/home	Oficio firmado por juez *	MLAT
https://legalrequests.twitter.com	MLAT	MLAT
https://leportal.microsoft.com/home	Oficio firmado por juez *	MLAT
https://safety-enforcement.tiktok.com/	Oficio firmado por juez *	MLAT
https://less.snapchat.com/?lang=ex-ES	Oficio firmado por juez *	MLAT
https://app.kodexglobal.com/	Oficio firmado por juez *	MLAT

*** En sistemas acusatorios aceptan que los pedidos estén firmados por el/la fiscal del caso, pero ocurre en la práctica que al realizarse así solo brinden datos de la creación de la cuenta.**

Fuente: Elaboración propia.

Cabe aclarar que las políticas de las ISP se van modificando, por lo que es de buena práctica actualizar con frecuencia los requisitos exigidos por cada una.

A continuación se comparte un ejemplo de requerimiento de información suministrada del usuario realizado a Facebook.



Fuente: Elaboración propia.

Todo sobre las direcciones de IP

DIRECCIÓN IP

Dirección de protocolo de internet (*internet protocol*). Cada elemento que quiere comunicarse a través de internet necesita tener asignada una dirección IP, administrada por **ICANN**

ICANN

- Corporación de internet para asignación de IP y dominios.
- Delega por regiones la administración de los bloques de las direcciones IP: A. del Norte, A. del Sur, Caribe, Asia, África y Europa.

Luego, cada región asigna a cada país un bloque de IP.

Cada país las distribuye entre las diferentes empresas proveedoras de servicio.

Las ISP las asignan a otros clientes particulares y empresas.

Claro | movistar | TELECOM | personal flow | Telecentro | iplan

ESTÁTICA
El cliente siempre mantendrá en el tiempo la misma dirección IP.

DINÁMICA
Cambia en el tiempo. Una dirección IP que un cliente tuvo asignada en un momento determinado es asignada a otro cliente de esa empresa en otro momento.

Por eso, en una investigación es necesario conocer, además de la dirección IP, la fecha, la hora y la zona horaria del evento asociado a esa dirección IP, para poder así solicitar al proveedor de servicios de internet los datos de abonado del cliente que tenía esa IP.

¿CÓMO SABER A QUÉ EMPRESA SOLICITO LA INFORMACIÓN DE UNA IP INVESTIGADA?
ALGUNOS SITIOS PARA CONSULTAR A QUÉ PROVEEDOR DE SERVICIO PERTENECE SON:
WWW.IPLOCATION.NET / WHOIS.LACNIC.NET

Fuente: Elaboración propia.

¿Qué hacer con la información recibida de las empresas internacionales?

Con la información recibida por parte de la ISP, se debe averiguar quién está detrás del usuario investigado, solicitando a la empresa nacional que administra esa dirección IP que informe los datos de abonado de ese usuario, es decir, los datos del cliente al que le fue asignada esa dirección IP —dinámica o estática (ver recuadro)— en ese preciso día y horario. No es necesario que dicho requerimiento sea realizado por el juez, como cuando se solicitan los datos de tráfico a las empresas internacionales. Al tratarse de datos de abonados, que contienen información menos sensible, son comúnmente solicitados por el fiscal o policía especializado.

Es fundamental ser exactos con la solicitud, pues si no se pide correctamente, se corre el riesgo de allanar un domicilio que no sea el del sospechoso.

Por lo tanto, la secuencia de la interpretación de la información que otorga la empresa internacional para efectuar correctamente el requerimiento a la compañía telefónica local es el siguiente:

1. Averiguar a qué empresa telefónica fue asignada la IP informada: ingresar a la página web del Registro de Direcciones de Internet para América Latina y Caribe (LACNIC) y colocar el número de IP. Inmediatamente esta arrojará el nombre de la empresa local a la que se asignó esa IP y, por ende, a quien se debe solicitar la información para identificar al sospechoso (Telecom, por ejemplo).
2. La fecha informada por la empresa internacional no indicará el momento en que el sospechoso se conectó o logueó para cometer el delito. La lectura de ella debe ser cuidadosa, pues es emitida por una empresa estadounidense y, por ende, debe invertirse el día y el mes (ver ejemplo).
3. Al horario informado en formato UTC hay que convertirlo al horario local. En la Argentina, se deben restar 3 horas, ya que el huso horario argentino es UTC-3[19].
4. La pregunta que se deberá efectuar a la empresa local será a quién se le asignó esa IP, ese día y horario —ya convertido—; es decir, los datos de abonados: nombre y apellido, domicilio, datos de contacto, el estado de cuenta y el tiempo que lleva como cliente. Este último dato es fundamental para a asegurar que el sospechoso viviera en ese domicilio durante el período en el que se habría cometido el delito.

En consecuencia, esta información permite dar con el lugar físico de conexión del usuario investigado que se habría conectado con el niño, niña o adolescente, o desde dónde había distribuido, facilitado o comercializado imágenes o videos de explotación sexual de NNyA. Luego, se deberá vincular dicho domicilio a un usuario o a una persona física.

Lo explicado se ejemplifica en la Figura 4.

19. Cabe señalar que las empresas extranjeras informan en distintos husos horarios (UTC, GMT, PDT, EST, EDT), el que se deberá determinar previo a realizar la conversión horaria al horario local. A fin de conocer correctamente cómo realizar esta conversión según el huso horario informado por cada empresa, se recomienda visitar https://www.worldtimebuddy.com/ .

Figura 4. Interpretación de la información de la ISP

Fuente: Elaboración propia.

Tareas de constatación

El siguiente paso consiste en determinar si el sospechoso vive en el lugar informado por la empresa nacional (Telecentro, por ejemplo) cuya IP fue aportada por la empresa internacional (Facebook, por ejemplo), como así también el lugar desde donde habría contactado al NNyA o generado el tráfico de material de explotación sexual de NNyA.

La empresa nacional informa al fiscal o policía especializada el/los domicilio/s de conexión del usuario sospechoso. Luego se ordena a las fuerzas policiales especializadas que realicen discretas tareas de constatación en el domicilio informado por la ISP. El objetivo es corroborar si el titular de la conexión informada por la empresa efectivamente reside allí y, en ese caso, qué otras personas viven en el lugar.

A su vez, a partir de esa información se intentará determinar si existe algún tipo de coincidencia entre el usuario investigado y los habitantes de ese inmueble. Por ejemplo, alguna fecha de nacimiento, el nombre de alguno de los habitantes que coincida parcialmente con el nombre de usuario, datos con los que se registró al abrir las cuentas en Facebook o Instagram, etc.

Figura 5. Pasos a seguir luego de obtener el domicilio de conexión

Fuente: Elaboración propia.

Allanamiento

A esta altura, el fiscal investigador puede tener serios indicios de que el autor del delito investigado vive en determinado lugar. En consecuencia, solicitará al juez el allanamiento de la morada y, en caso de considerar que corresponde, el juez emitirá la orden de allanamiento sin descuidar la importancia de secuestrar y registrar dispositivos de almacenamiento informático que, seguramente, contienen la evidencia digital que implicará al sospechoso.

No es lo mismo realizar un allanamiento para secuestrar prueba física (estupefacientes, por ejemplo) que evidencia digital (registrar fotografías o videos de abuso sexual de niños, niñas y adolescentes, o conversaciones entre el *groomer* y eventuales víctimas). Así, cuando culmine el primero, se podrá determinar inmediatamente si se encontraron o no los elementos provenientes del delito investigado. Sin embargo, no ocurrirá lo mismo cuando termine el procedimiento para registrar la evidencia digital.

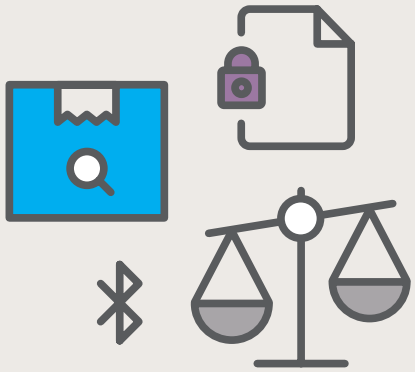
Ello es porque si bien se incautan objetos (computadoras, teléfonos celulares, *tablets*, *pendrives*, etc.), lo que se busca son los datos que contienen aquellos objetos. Entonces, cuando se termine el allanamiento no se tendrá conocimiento de si lo que se busca está efectivamente en el material incautado, porque el verdadero registro se llevará a cabo en el laboratorio forense. Es así salvo algún caso en el que, excepcionalmente y por motivos de extrema gravedad, se decida efectuar el registro en el lugar.

Es necesario que el pedido de allanamiento del fiscal al juez incluya los puntos técnicos de análisis, como así también la modalidad de registro de esos datos: copia o imagen forense (*bit* a *bit*) para posterior análisis, o bien análisis en el lugar —*triage* o búsqueda rápida— para casos en los que pueda existir un riesgo concreto por la presencia de niños o niñas conviviendo con el sospechoso.

También, durante el allanamiento es fundamental el modo en el que se secuestran los objetos materiales dentro de los cuales se encuentran los datos que se quiere obtener. Allí se inicia la cadena de custodia. El procedimiento que se sigue hasta la presentación del informe técnico deberá ordenarse con miras a su presentación en el juicio oral y público.

Por ello, en las próximas páginas se explicará, en detalle, cómo se realiza la identificación, resguardo y extracción de la evidencia digital durante el allanamiento, y el análisis de aquella en el laboratorio informático.

Obtención y preservación de evidencia digital: protocolo de buenas prácticas



Las pruebas o evidencias digitales se refieren a cualquier información almacenada o transmitida electrónicamente que pueda utilizarse en procedimientos judiciales. Entre ellas, se encuentran los correos electrónicos, metadatos, documentos digitales, datos de geolocalización GPS, registros de chats, imágenes y grabaciones de videos que suelen almacenarse en dispositivos personales o plataformas de terceros, como redes sociales y servicios en la nube[20].

Se trata de registros que fueron procesados en un dispositivo informático y se encuentran almacenados o fueron transmitidos a través de un medio de comunicación informático (Presman, 2018:304).

Para la recolección y posterior tratamiento de la evidencia digital es fundamental atender a protocolos específicos. En ese sentido, la *Guía para la identificación, recolección, adquisición y preservación de la evidencia digital*, de la International Organization for Standardization (ISO), presenta normativa metodológica para la escena del hecho y procedimientos de recolección y tratamiento de la evidencia digital.

Por otro lado, el protocolo elaborado por el Instituto Nacional de Justicia del Departamento de Justicia de Estados Unidos[21] fue especialmente preparado para asistir al personal de las fuerzas de

20. Para más información, ver las Directrices para fiscales sobre la recopilación de las pruebas digitales de la UNESCO y el International Association of Prosecutors. pág. 4.
21. Para más información, visitar: Electronic Crime Scene Investigation, A Guide for first responders. http://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

la ley y a las y los responsables de identificar y preservar dispositivos que contengan evidencia digital en el lugar del hecho. El documento establece una clasificación de diversas fuentes de evidencia digital, proporciona lineamientos para la recolección de material probatorio, manejo de cadena de custodia y otras consideraciones especiales sobre evidencia digital.

Más allá de las guías de buenas prácticas, la recolección de evidencia digital no es un proceso lineal que siempre se hace de la misma forma; las metodologías pueden diferir unas de otras en diferentes casos.

Sin embargo, siempre es fundamental respetar la cadena de custodia. Se trata de llevar un registro minucioso de cada movimiento de la evidencia en un proceso probatorio. Este indica con exactitud las actividades realizadas, las personas que intervinieron y el estado de la evidencia. Es el conjunto de documentos sobre los elementos de prueba que permitirán asegurar y demostrar la identidad, integridad y registro de la evidencia digital (Presman, 2018:308).

Evidencia digital

Según Presman, algunas características propias de la evidencia digital a considerar son:

- Está conformada por un conjunto de *bits*, la mínima expresión de almacenamiento que solo puede tener un valor binario: cero o uno. Esta característica es clave en el sentido de que todo registro digital puede ser duplicado y las copias que se realicen del mismo, si siguen las buenas prácticas, serán idénticas e indistinguibles del original.
- Es intangible; el disco rígido es el envase que soporta a los *bits* de información allí almacenada.
- Posee metadatos; esto es, el dato del dato, por ejemplo, la fecha de creación del documento.
- Permite almacenar grandes volúmenes de información en contenedores de dimensiones reducidas, como es un disco rígido, circunstancia que exige una correcta identificación para no perder evidencia valiosa (Presman, 2018:304-5).

Inadmisibilidad

En Estados Unidos, las normas procesales federales requieren que la parte que solicita la incorporación al proceso de pruebas digitales demuestre su autenticidad acreditando el respeto de la cadena de custodia. El incumplimiento de esta exigencia puede determinar la inadmisibilidad de la evidencia[22].

Cadena de custodia

Un elemento central para poder utilizar la evidencia material o digital en un juicio, especialmente aquella que fue obtenida en el lugar allanado, es que haya sido recogida por un funcionario especializado, conforme al protocolo y procedimiento establecido para ello, y que haya sido preservada, exenta de manipulación (Cristoldi *et al.*, 2025).

En ese sentido, la cadena de custodia es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos y evidencia digital que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal. Debe garantizar que la evidencia que se presenta en el juicio sea exactamente la misma que ha sido secuestrada, preservada, copiada y analizada, y que no sufrió adulteraciones o modificaciones (Caballero, 2021).

Significa garantizar que desde que se recogen los vestigios que se relacionan con el delito hasta que llegan a concretarse como prueba en el momento del juicio oral, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio del tribunal, es lo mismo (Chia, 2020:278-9). Es decir, es el procedimiento necesario para tener la seguridad de que lo que se traslada, analiza o se visiona es lo mismo desde que se interviene hasta el momento final que se estudia[23].

La cadena de custodia le permite al juez saber y dar por cierto que la evidencia digital que es presentada en el juicio por los litigantes (fiscales y defensores a través de sus testigos) no ha sido adulterada, cambiada o modificada de modo alguno desde que se la recogió.

Para llevar adelante esa actividad es preciso acreditar tanto el método utilizado como el personal que lo llevó a cabo. Si el método es incorrecto, el almacenamiento inadecuado o la persona incapaz de cumplir su cometido, el trabajo será inútil y la evidencia inservible (Chia, 2010).

22. Para más información, ver United State v. Salcido, 506 F.3d 729,733, Corte Federal de Apelaciones del 9no. Circuito, 2007, citado en Blanco, Hernan, Tecnología informática e investigación criminal, Bs.As., Thomson Reuters, La Ley, p. 748, 2020.
23. SSTS 6/2010, de 27 de enero, 776/2011, del 20 de julio.

Por ello, para la recolección y posterior tratamiento de la evidencia digital es fundamental atender a protocolos específicos.

La cadena de custodia es la historia cronológica de la evidencia digital y material relatada por el o los testigos expertos, desde que es recogida hasta que llega a juicio oral.

Integridad y autenticidad

Garantizar la integridad y autenticidad de las pruebas digitales es un requisito fundamental para su admisibilidad en los procedimientos judiciales, pues están intrínsecamente ligados al valor probatorio del material digital y deben salvaguardarse mediante protocolos forenses rigurosos.

La **integridad** es la garantía de que los datos digitales no han sido alterados desde el momento de su recopilación hasta su presentación ante el tribunal.

La **autenticidad** se refiere a la capacidad de demostrar que las pruebas proceden de una fuente verificable.

Pasos fundamentales a seguir

Como orientación para los investigadores y litigantes, en este apartado se comparten algunas pautas del Protocolo de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas de Ciberdelitos[24], y de los protocolos referidos y comentados en la *Guía práctica para un abordaje integral del ciberdelito* ya citada para la identificación, selección, secuestro y preservación de la evidencia digital, así como los principales pasos para el tratamiento de la prueba electrónica.

24. Res. 2347/2016. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-234-2016-262787

En ese sentido, es muy importante el cumplimiento por parte de la policía especializada de los siguientes pasos y su consiguiente comprobación a través de las declaraciones de los expertos en el juicio:

1. Asegurar la escena

Implica resguardar el área en la que ocurre el evento informático y los elementos materiales probatorios que se encuentren allí. Se debe evitar el acceso de personal extraño al área, así como la utilización de los equipos informáticos allí existentes.

2. Identificación

Antes de comenzar la recolección de pruebas digitales, el investigador debe definir los tipos de prueba que busca[25].

Las pruebas digitales pueden encontrarse en dispositivos digitales, computadoras, monitores, teclados, parlantes, discos externos, *mouses*, módems, *routers*, impresoras, *scanners*, micrófonos (por las huellas digitales y ADN), CD, *pendrives*, tarjetas de memoria, discos rígidos y externos, celulares, *smartphones*, *tablets*, GPS, videocámaras, consolas de videojuego y cualquier otro dispositivo que pueda tener evidencia digital o IoT, como *smart watches*, heladeras, asistentes tecnológicos, etc. Muchas aplicaciones, sitios web y dispositivos digitales utilizan servicios de almacenamiento en la nube, por lo que los datos de los usuarios pueden ser acopiados en su totalidad o en fragmentos en muchos servidores diferentes situados en múltiples lugares.

Dado que los investigadores pueden encontrarse con múltiples dispositivos digitales, sistemas operativos y complejas configuraciones de red, esto requerirá conocimientos especializados, variaciones en los procedimientos de identificación y recolección, y asistencia para identificar conexiones entre los sistemas y dispositivos.

La diversidad de dispositivos digitales, sistemas operativos y configuraciones de red demanda conocimientos especializados y procedimientos rigurosos para identificar las conexiones entre cada componente.

3. Recolección

La recolección real de las pruebas implica conservar las pruebas volátiles y apagar los dispositivos digitales. El estado de operatividad de los dispositivos de almacenamiento informáticos encontrados, y los tipos de dispositivos digitales que se secuestren, determinarán el procedimiento de recolección.

25. Para más información, visitar: cfr. *Ciberdelitos II. Guía práctica para un abordaje integral del fenómeno.* UNODC, Modulo 6, ps. 18 y ss.

Se comparten aquí algunas de las recomendaciones de cara al juicio oral; de acuerdo al dispositivo electrónico variará su tratamiento:

- Fotografiar el estado en el que se encuentra el dispositivo cuando se lo halló y cuando se lo secuestra, por si ha habido un cambio en su pantalla.
- Desconectar y etiquetar el cable de suministro y demás cables o dispositivos USB conectados a la computadora.
- No encender nunca un equipo apagado. Si está encendido, no apagarlo inmediatamente para evitar la pérdida de información volátil.
- Verificar lo que muestra la pantalla del dispositivo electrónico para detectar si se está accediendo a él remotamente o bien si la información está siendo destruida.
- Si es una computadora de escritorio: a) Si el monitor está encendido, sacar una fotografía a la pantalla y registrar lo que se ve; b) Si el monitor está encendido, pero se ve el protector de pantalla, mover ligeramente el *mouse* sin tocar ningún botón ni mover la rueda; c) Si el monitor está apagado, pero el gabinete está encendido, prender el monitor, fotografiar la pantalla y registrar la información que aparezca; d) Si el monitor está encendido, pero la pantalla está en negro, como si estuviera apagada, mover ligeramente el *mouse*.
- Si fuera una *laptop* o computadora portátil, se recomienda mover el cable de alimentación, localizar y remover la batería.
- En caso de dispositivos móviles y celulares, si el aparato está encendido, no apagarlo y si está apagado, dejarlo apagado.

4. Embalaje

Cada dispositivo debe ser etiquetado, junto con sus cables de alimentación, empaquetado y transportado al Laboratorio de Análisis Forense. Para ello es importante considerar:

- La evidencia digital es frágil y sensible a altas temperaturas, humedad, electricidad estática y campos magnéticos.
- Embalar toda la evidencia digital en bolsas antiestáticas y no utilizar material plástico.
- Todo lo que pertenezca a una computadora será identificado o rotulado, embalado y transportado en su conjunto para evitar que se mezcle con otros dispositivos.
- Fajar con fajas de papel y pegamento los puertos y todas las entradas, de manera que no se puedan remover o reemplazar las piezas internas.

5. Transporte

Documentar quiénes participaron del empaquetamiento y transporte para registrar la cadena de custodia.

6. Almacenamiento

Realizar un inventario de toda la prueba y almacenarla en un ambiente seguro, sin altas temperaturas ni humedad. La evidencia no debe estar expuesta a campos magnéticos, humedad, polvo o cualquier elemento que pueda dañarla o destruirla.

7. Documentación

Todo lo realizado durante el proceso de recolección, transporte y almacenamiento de las evidencias tiene que estar documentado, preservado y disponible para un posterior examen. Esta documentación debe incluir información detallada sobre los dispositivos digitales de los que se

extrajeron las pruebas, el *hardware* y el *software* utilizados para obtener dichas evidencias, cómo, cuándo, dónde y porqué se obtuvieron (Maras, 2014).

8. Aseguramiento

Existen diferentes métodos, y dependerá del tipo de dispositivo electrónico, pues el procedimiento para obtener y preservar pruebas del disco duro de una computadora es diferente del procedimiento requerido para obtener evidencia de los celulares. A menos que se realice una obtención en vivo, las pruebas se extraerán en el laboratorio forense (obtención estática). Se debe garantizar la utilización de herramientas forenses que aseguren la integridad y conservación de las pruebas, de manera que los datos no se alteren. Las herramientas y técnicas utilizadas deben ser válidas y fiables (SWGD, 2018).

Es importante resaltar que la información se asegura y preserva, antes que nada, haciendo un duplicado del contenido de dicho dispositivo —se obtiene así una imagen o copia forense— y el analista trabaja en la copia sobre los puntos a analizar.

Para verificar si el duplicado es una copia exacta del original se calcula un valor de *hash* criptográfico para el original y el duplicado mediante cálculos matemáticos. Ambos valores —del original y de la copia— deben coincidir para determinar la inalterabilidad de los datos[26].

9. Análisis y presentación de informes técnicos

La evidencia digital será examinada y analizada por personal idóneo, entrenado y capacitado para ese propósito, en base a los puntos solicitados por el fiscal.

El proceso de análisis forense digital implica evaluar e interpretar la información (*fase de análisis*) y comunicar los resultados del análisis (*fase de presentación de informes*). En la primera fase, es fundamental que el investigador pueda coordinar con el analista forense los puntos de pericia[27].

En la fase de la presentación de resultados, los informes deben ser claros y precisos; pueden incluir material demostrativo y documentos de apoyo. Los hallazgos deben explicarse a la luz de los objetivos del análisis (propósito de investigación), dejando asentadas debilidades y fortalezas. Este informe será utilizado para refrescar la memoria del perito o establecer inconsistencias, en caso de que el analista diga algo distinto a lo que incluyó en el informe técnico.

Lo señalado en los puntos 1 a 7 se lleva a cabo en la morada allanada y en el transporte al laboratorio informático por parte del personal especializado, por orden del juez y a pedido del fiscal. Los pasos 8 y 9, se desarrollan en el laboratorio informático.

26. El *hash* es la huella digital de la información electrónica que permite comprobar que no se alteró la prueba original. Asegura la autenticidad e integridad de la prueba digital, posibilitando determinar que esa evidencia contenida en el dispositivo secuestrado es la misma que la copiada, sin alteraciones.
27. Para más información, visitar: cfr. Ciberdelitos II. Guía práctica para un abordaje integral del fenómeno. UNODC, Modulo 6, ps.25/28.

Debates sobre el aseguramiento y la extracción de evidencia digital

Una de las principales discusiones que se suscitan antes de analizar los dispositivos secuestrados es si al momento de efectuarse el aseguramiento de la imagen forense[28] —o copia *bit* a *bit*— es necesaria la presencia de la defensa.

Esto dependerá de si ese acto se concibe como irreproducible o no. En este sentido, diversos especialistas sostienen que la clonación o la copia de la evidencia digital que se encuentra en el dispositivo de almacenamiento informático del sospechoso es una medida reproducible, dado que se pueden hacer tantas copias como sean necesarias, siempre que se utilicen herramientas forenses que garanticen (mediante un valor *hash*) la inalterabilidad del original[29].

La Cámara Nacional de Apelaciones Criminal y Correccional, Sala IV[30] ya se expidió al respecto y, en idéntica línea, se pronunció TS de España[31].

No obstante, en la práctica es común notificar a la defensa de su realización para demostrar que el procedimiento garantiza la cadena de custodia de los elementos secuestrados y cuya copia se efectuará, como así también con el fin de evitar futuros planteos que puedan dilatar el trámite del caso.

Luego de ello, puede ocurrir que los peritos informáticos de ambas partes analicen la evidencia digital en forma conjunta, o bien que se realicen copias para que las analicen individualmente los técnicos de cada parte. Luego se presentarán y controlarán sus resultados a través del examen y contra examen de los peritos informáticos en el debate oral.

28. La imagen forense es la copia a un disco de la evidencia digital que se encuentra en el original que, por medio de un *hash* se confirma que el contenido del disco no ha sufrido cambio alguno; En: Velázquez, Andrés, Los próximos paradigmas de las pruebas digitales, en Cibercrimen II, dir. Dupuy, D., coord. Kiefer, M., B de F, Buenos Aires, 2016, p. 314 y ss.
29. En este sentido ya se expidió TS Español, Sala de lo Penal. Madrid. 767/2019, 12 de septiembre.
30. Cámara de Apelaciones en lo Criminal y Correccional, Sala IV, causa A, J. A. y otros s/nulidad: la apertura de los teléfonos celulares es valorada por el Tribunal como la obtención de una copia de la información que obraba en los aparatos, es decir, la guarda de un soporte informático de los datos que estaban almacenados en el dispositivo... La omisión de notificar a la defensa no acarrea la nulidad del acto.
31. TS Sala de lo Penal. Madrid. 767/2019, 12 de septiembre: Como recientemente recordamos en nuestra Sentencia 388/2018, de 25 de julio , hemos de indicar que esta Sala ha considerado que no es necesario que esté presente en la diligencia de volcado o clonado de datos el Letrado de la Administración de Justicia (STS 342/2013, de 17 de abril ; o STS 165/2016, de 2 de marzo) y el nuevo artículo 588 sexies c) de la LECRIM no lo exige (cuando regula el acceso a la información contenida en instrumentos de comunicación telefónica, entre otros). Tampoco se ha considerado necesaria la presencia del interesado o su Letrado (STS 342/2013, de 17 de abril), porque ni la ley procesal anterior al año 2015 ni tampoco la nueva normativa de la Ley de Enjuiciamiento Criminal (Ley 13/2015, de 5 de octubre) imponen que estén presentes el letrado del imputado ni un perito nombrado por la parte en el momento de volcar el contenido del ordenador. Es más, el nuevo artículo 588 sexies c) ni siquiera requiere la presencia del secretario judicial en el momento de abrir el ordenador y obtener el disco duro. Y en cuanto al nombramiento de un perito de parte para que esté presente, la sentencia de esta Sala 342/2013, de 17 de abril, si bien considera que la parte puede designar un perito, de acuerdo con lo dispuesto en el art. 476 de la LECr. su no intervención no condiciona la validez de la diligencia (STS 165/2016, de 2 de marzo).

Otro eje de discusión refiere a si la extracción de información digital o la obtención de imágenes forenses constituye o no un acto pericial. Aunque esta cuestión generó debates en el pasado, la jurisprudencia internacional ha tendido a resolver mayoritariamente que la mera obtención de la copia forense no integra en sí misma un peritaje, sino que constituye una etapa previa y técnica destinada a posibilitar la labor pericial posterior (Polansky, 2023).

Los pasos señalados sirven de guía para llevar a cabo un examen directo en el juicio de quienes participaron en dichos escalones, y para que la contraparte efectúe un control exhaustivo de ello.

Si las partes desconocen las bases de este u otros protocolos o guías internacionales, no podrán demostrar correctamente la adquisición de la evidencia, ni saber si los expertos de la contraparte lo hicieron correctamente.

En consecuencia, los investigadores, los técnicos de la escena del delito, o los expertos en el análisis forense digital deben demostrar que no se modificaron las evidencias digitales durante la fase de identificación, recolección y obtención, dependiendo de los dispositivos (computadoras o celulares, por ejemplo), exhibiendo en el paso a paso el respeto de la cadena de custodia.

Cada fase debe explicarse al detalle en el juicio oral, demostrando su intangibilidad y trazabilidad desde el primer momento hasta la entrega del informe técnico a las partes.

Requisitos de admisibilidad de la evidencia digital

Para garantizar la admisibilidad de las evidencias digitales deben cumplirse ciertos requisitos legales y técnicos.

En cuanto a los **legales**, se encuentran:

- La autorización legal para llevar a cabo registros e incautaciones de los datos contenidos en los dispositivos electrónicos. El juez verificará y la contraparte controlará si el fiscal utilizó la autorización legal apropiada (orden de registro) para registrar e incautar los datos provenientes de las TIC.
- La pertinencia forense se determina según si las pruebas digitales vinculan o descartan una conexión entre el autor y el objetivo de la investigación, o la escena del delito, por ejemplo.
- La integridad y fiabilidad de las evidencias digitales se evalúa examinando los procedimientos y herramientas forenses utilizados para obtener las pruebas digitales, la competencia y las calificaciones de los expertos forenses digitales que las han obtenido, conservado y analizado.

En relación a los **técnicos**, se pondrá énfasis:

- En los procedimientos e instrumentos de análisis forense digital utilizados para extraer, conservar y analizar la evidencia digital.
- En los laboratorios digitales donde se realizan los análisis.
- En los informes de los analistas forenses digitales, y en las calificaciones técnicas y académicas de dichos analistas.

Consideraciones y recomendaciones

A continuación se detallan algunas consideraciones y recomendaciones a tener en cuenta durante las investigaciones en entornos digitales.

- El fiscal deberá explicar cómo llegó, durante la investigación, al domicilio del acusado. Esta explicación debe ser desarrollada paso a paso y desde el primer momento.
- Algunos testigos suelen ser investigadores propios de la fiscalía. Son ellos quienes conocen los procedimientos a seguir para preservar la evidencia digital y son quienes deberán explicar por qué esa evidencia —preservada— no es otra, es decir, no fue alterada. Dicha presentación pormenorizada de todo lo investigado facilita el entendimiento de los jueces.
- Para preservar la evidencia no es necesario ser técnico ni informático; un investigador entrenado puede realizarlo y explicarlo al tribunal durante el juicio. Es fundamental que el juez conozca en qué consiste la preservación de evidencia digital, pues ello le permitirá validar o no lo manifestado por quien la realizó.
- Los analistas o técnicos deben poder demostrar a través de sus exámenes tanto si utilizaron principios científicos para obtener, conservar y analizar la evidencia digital como si las herramientas forenses utilizadas son validadas internacionalmente, actualizadas, mantenidas adecuadamente y probadas antes de su uso para garantizar el funcionamiento correcto. Un juez debe esperar que el fiscal lo examine en ese sentido, para nutrirlo de información de calidad.
- Los expertos deberán ilustrar acerca de cómo funcionan los dispositivos digitales, las plataformas en línea, el proceso de análisis forense digital, por qué se utilizó una herramienta y no otras, cómo se conservaron y analizaron las evidencias, la exactitud de estas interpretaciones y cualquier alteración que se pudo producir en los datos y el motivo. En el marco de un sistema acusatorio, el juez debe pretender que el fiscal le haga todas las preguntas necesarias al informático para luego poder recibir la información detallada.
- El fiscal deberá poner énfasis en la acreditación correcta de los analistas forenses, para garantizar la calidad de los productos y la confianza en los resultados obtenidos.
- El uso de protocolos para preservar la evidencia digital es fundamental: la demostración de que en todos los casos hay un idéntico proceder trazable e inalterable para su conservación es información de alta calidad y utilidad para los jueces. Se debe dejar plasmado que el laboratorio utiliza métodos fiables, equipos y programas informáticos adecuados, y personal competente.

- La utilización de videos demostrativos y gráficos resulta un complemento indispensable mientras se desarrolla el examen del testigo que realizó la preservación. Ello le permite al juez tomar una dimensión más clara de la complejidad del fenómeno.
- Los jueces y los fiscales deberán saber que no se encontrará presente en el juicio ningún representante de Facebook, Microsoft o Google que se expida acerca del contenido de la información brindada. Los informes entregados por estas compañías carecen de firma y se reciben por canales informales. ¿Ello podría representar un problema? Si se llegó a un acuerdo entre las partes para incorporarlos, no. De lo contrario, la defensa podría sembrar dudas acerca de su origen y legitimidad.
- La conversión horaria no es sencilla de explicar; el uso de gráficos por parte de testigos es fundamental y su procedimiento deberá ser irrefutable para que al tribunal no le quede duda alguna de la vinculación de los datos iniciales con el domicilio de conexión utilizado para delinquir.
- Usar gráficos es un excelente método para apoyar el relato y que el tribunal mantenga su atención. Asimismo, complementa una explicación técnica que suele tener cierto nivel de dificultad.
- La demostración en tiempo real ayuda a que el tribunal comprenda bien la evidencia que se le presenta. Si el imputado por distribuir videos de abuso sexual de NNyA se valió de una red P2P, como el *software* E Donkey, el fiscal deberá examinar a su testigo experto sobre qué es y cómo funciona esa red para compartir. Seguramente, si el técnico lo explica, al tribunal le costará entenderlo a la perfección. Así, una estrategia a la que puede acudir el litigante, previa solicitud de autorización al tribunal, es que el testigo explique la herramienta utilizada por el imputado para cometer el delito mientras efectúa una demostración en tiempo real acerca de su funcionamiento y alcance, accediendo para ello a internet y al *software* específico para la demo.
- Los litigantes deberán asegurarse, con antelación, que tendrán posibilidad de proyectar en la sala de juicio y contarán con acceso a internet para cualquier demostración en vivo que sea necesario exhibir para una mejor comprensión.
- La trazabilidad y explicabilidad son dos objetivos fundamentales a la hora de examinar a los testigos e ir armando una línea completamente trazable y explicable del principio al fin.
- Los alegatos de clausura constituyen el momento de relacionar toda la prueba producida en el juicio, vincularla con el alegato de apertura y concluir los resultados obtenidos de manera clara, concreta y sin perder ningún eslabón de nuestra teoría del caso. Es momento de que los litigantes expliquen al tribunal, en lenguaje llano, cómo y cuándo se cometió el delito en el ciberespacio, y de qué manera se arribó a los resultados obtenidos, incluyendo cómo se preservó, se extrajo, se analizó y se procesó la evidencia electrónica. Para ello pueden usarse presentaciones en PowerPoint o Prezi.
- La formación de los jueces y fiscales es fundamental para litigar este tipo de casos, cuya nueva lógica no es "lo que vendrá"; ya que está aquí, entre nosotros, para investigar y litigar cualquier delito.

GLOSARIO

Acta de secuestro: Documento legal que certifica la incautación de un dispositivo.

Admisibilidad: Estado de la evidencia digital para ser incorporada válidamente al proceso judicial, siempre que haya sido obtenida conforme a las normas legales y procesales vigentes.

Asistente técnico en informática: Personal que colabora con los profesionales en la gestión interna de elementos probatorios que requieran para las actividades operativas y le deriva a estos las consultas sobre pericias que estén en trámite.

Autenticidad de la evidencia: Capacidad de demostrar que la prueba no fue alterada. Se protege el material probatorio mediante etiquetas de seguridad y la debida diligencia de la cadena de custodia. No hay suplantación, manipulación o alteración indebida.

Bloqueador de escritura: Dispositivo de *hardware* o *software* que impide cualquier modificación física o lógica en el soporte original durante el proceso de extracción de datos, garantizando la integridad de la evidencia.

Bolsa de Faraday: Elemento de protección utilizado para aislar dispositivos móviles de cualquier conexión de red (Wi-Fi, *bluetooth*, telefonía u otras) y prevenir accesos remotos, alteraciones o bloqueos.

Bolsa de seguridad: Embalaje inviolable que evita daños al material probatorio. Se debe usar siempre para discos.

Cadena de custodia: Conjunto de procedimientos administrativos y legales que garantizan la autenticidad, integridad y trazabilidad de la evidencia digital, registrando a cada persona que tuvo contacto con ella y las circunstancias de tiempo, modo y lugar.

Ciberespacio: Conjunto de infraestructuras tecnológicas, redes de datos, sistemas informáticos y plataformas digitales que permiten que personas, organizaciones y dispositivos se conecten e interactúen entre sí a través de internet. Incluye desde páginas web, aplicaciones y redes sociales hasta servicios en la nube, sistemas críticos y dispositivos conectados.

Clonación de disco: Copia exacta de un disco. Si se hace fuera del laboratorio se debe verificar si cuenta con un valor *hash* asociado que sea informado.

Copia (o imagen) forense: Copia *bit a bit* de un dispositivo digital que permite obtener una réplica exacta del contenido original para su análisis, sin modificar el medio de origen. La realizan los peritos. Al finalizar el proceso se genera un valor *hash* que garantiza la integridad de los contenidos digitales. Ambas expresiones son válidas: copia forense e imagen forense.

***Dark web*:** Conjunto de servicios y sitios accesibles exclusivamente mediante redes de anonimización, caracterizados por el ocultamiento de direcciones IP, el cifrado de las comunicaciones y la alta volatilidad del contenido.

Disco rígido: Dispositivo electromecánico de almacenamiento de información digital.

Embalaje forense: Técnicas de protección física de evidencias. Se utilizan materiales adecuados (bolsas, cajas, sobres) y etiquetas de seguridad.

Evidencia volátil: Conjunto de datos digitales que pueden perderse, alterarse o modificarse al apagar el dispositivo o cambiar su estado operativo, incluyendo memoria RAM, procesos en ejecución, sesiones activas y conexiones de red.

Función *hash* (MD5, SHA-1, SHA-256): Algoritmo criptográfico utilizado para generar un valor de verificación único sobre la información extraída, permitiendo comprobar que la evidencia digital no ha sido alterada. Se conserva como referencia de integridad.

***Logs* de conexión:** Archivos o registros que almacenan datos sobre cuándo, desde dónde y cómo un usuario o dispositivo se conecta a un sistema, plataforma o red. Son esenciales para fines de seguridad informática, auditoría, trazabilidad y cumplimiento normativo.

Metadatos: Información secundaria asociada a archivos o registros digitales —como fechas de creación, modificación, autor o actividad— que puede verse alterada por intervenciones mínimas no controladas. Información oculta de un archivo con atributos especiales que aporta detalles técnicos.

Noticia criminis: Información inicial que alerta a las autoridades sobre un hecho que podría constituir un delito, dando fundamento para iniciar una investigación preliminar o una causa penal.

Precinto de seguridad: Sello numerado inviolable que debe registrarse en el Sistema de Gestión de Laboratorio y en actas de entrega de material probatorio.

Preservación: Conjunto de medidas técnicas, jurídicas y documentales destinadas a evitar la pérdida, alteración, destrucción o contaminación de la evidencia digital desde su identificación hasta su análisis pericial.

Quick freeze: Procedimiento de preservación inmediata y dirigida de datos (*traffic data*, como direcciones IP, números telefónicos o datos de localización), ordenado por una autoridad judicial cuando existe sospecha concreta de un delito. Su función es "congelar" temporalmente esos datos para evitar su eliminación, permitiendo que luego puedan ser solicitados formalmente ("descongelados") para su uso como evidencia en una investigación penal.

***Software* forense:** Programa de análisis forense digital.

Solicitud de preservación: Requerimiento formal dirigido a un proveedor de servicios digitales para que conserve temporalmente datos asociados a una cuenta, perfil o contenido, sin implicar su entrega inmediata ni su análisis.

Trazabilidad: Capacidad de reconstruir de manera completa, cronológica y verificable el recorrido de la evidencia digital desde su identificación y obtención hasta su presentación judicial, incluyendo responsables, procedimientos y lugares de intervención.

***Triage* digital:** Proceso de evaluación preliminar realizado sobre un sistema encendido con el fin de identificar y recolectar de forma rápida evidencia volátil o de interés inmediato.

Validez legal: Reconocimiento jurídico de la prueba. Depende de una cadena de custodia correcta.

Volatilidad: Característica de ciertos datos digitales —especialmente los alojados en una memoria RAM— que tienden a perderse o alterarse si el dispositivo se apaga o cambia su estado operativo.

Siglas

CSAM
Child sexual abuse material / Material de abuso sexual infantil.

DHS
Department of Homeland Security (Estados Unidos) / Departamento de Seguridad Nacional.

HSI
Homeland Security Investigations / Oficina de Investigaciones de Seguridad Nacional de los Estados Unidos, especializada en delitos transnacionales, entre ellos la explotación sexual infantil.

ID
Identificador único asignado a un usuario, cuenta o dispositivo.

IMEI
International mobile equipment identity / Es el código de identificación internacional del equipo de telefonía celular. Posee 15 dígitos y permite que un proveedor de servicio de telefonía pueda individualizar el aparato. Este código brinda información sobre el fabricante, modelo/tipo, etc.

IMSI
International mobile subscriber identity / Identificador único asignado a un abonado de telefonía móvil.

INTERPOL
International Criminal Police Organization / Organización Internacional de Policía Criminal.

IoT
Internet of things / Internet de las cosas.

IP
Internet protocol address / Dirección que identifica un dispositivo en una red.

ISP
Internet service provider / Proveedor de servicios de internet. En este trabajo se utiliza la sigla ISP para referirse también a empresas, plataformas digitales y redes sociales que operan en múltiples países y que permiten a las personas conectarse entre sí, y buscar, gestionar, compartir y almacenar información. Ejemplos típicos: Google, Meta, Microsoft, Apple, Cloudflare, TikTok, entre otros.

LAC
Location area code / Código que identifica un área geográfica dentro de una red móvil.

LACNIC
Registro de Direcciones de Internet para América Latina y Caribe.

MCC
Mobile country code / Código que identifica el país del operador móvil.

MNC
Mobile network code / Código que identifica al operador de red móvil dentro de un país.

MLAT
Mutual Legal Assistance Treaty / Tratado de asistencia jurídica mutua. Es un acuerdo bilateral o multilateral entre países que establece mecanismos formales de cooperación para obtener evidencia en investigaciones penales, solicitar registros, documentos o datos digitales y tramitar órdenes judiciales transfronterizas.

NCMEC
National Center for Missing and Exploited Children / Centro Nacional para Menores Desaparecidos y Explotados (ONG de Estados Unidos).

NNyA
Niños, niñas y adolescentes

OSINT (Open Source Intelligence)
Es un conjunto de técnicas y herramientas para recopilar, analizar y correlacionar información pública.

P2P
Peer-to-peer / Redes de intercambio de archivos entre pares (puerta a puerta).

URL
Uniform resource locator / Dirección web que permite acceder a un recurso en internet.

SIM
Subscriber identity module / Tarjeta que identifica al usuario en una red de telefonía móvil.

SWGD
Scientific Working Group on Digital Evidence / Grupo de trabajo científico sobre evidencia digital.

TIC
Tecnologías de la información y la comunicación.

TMSI

Temporary mobile subscriber identity / Identificador temporal utilizado para proteger la identidad del abonado en redes móviles.

UFED

Universal Forensic Extraction Device / Herramienta forense de extracción y análisis de datos digitales desarrollada por Cellebrite.

UFEDyCI

Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires.

UNODC

United Nations Office on Drugs and Crime / Oficina de las Naciones Unidas contra la Droga y el Delito.

VPN

Virtual private network / Red privada virtual que permite ocultar o modificar la ubicación y la dirección IP del usuario.

Bibliografia

- Chia, R. A. (2010). *La prueba en el proceso penal*. Bs.As.: Hammurabi
- Chía, R. A. (2020). *Técnicas de litigación penal*. Bs.As.: Hammurabi.
- Cistoldi. P., Di Iorio. A. y otros (2025). *Prueba digital: de la cadena de custodia a la cadena de valor.* En*: Tratado Procedimiento Criminal, Transnacional y Digital*, dirigido por Daniela Dupuy. Madrid: Tirant Lo Blanch.
- Caballero, O. G. (2021). *Examen y contraexamen de testigos y peritos*. Bs. As. Contexto.
- Di Iorio, A. (2016). Protocolos de preservación de evidencia digital y cuestiones forenses. Cibercrimen II, dirigido por Daniela Dupuy. Buenos Aires: BdeF.
- Dupuy, D. *et al.* (2022). *Acosos en la red a Niños, Niñas y Adolescentes*, Cibecrimen 1. Buenos Aires: Hammurabi.
- Dupuy, D. y Kiefer, M. (2020). La transferencia transfronteriza de datos en el marco de investigaciones criminales. *Revista Derecho y Nuevas Tecnologías*, N° 2. CETyS. Universidad de San Andrés. Dirigido por Pablo Palazzi.
- Maras, M. H. (2014). *Computer Forensics: Cybercriminals, Laws, and Evidenes.* Massachusetts: Jones & Bartlett.
- Miró Llinares, F. (2012). *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.
- Polansky, J. (2023). *Qué es y que no es un peritaje en el entorno digital*, en La investigación penal en el entorno digital. Bs. As.: Hammurabi.
- Presman, G. D. (2018). *La cadena de custodia en la evidencia digital*. Cibercrimen II, dirigido por Daniela Dupuy. Buenos Aires: BdeF.
- SWGD (2018). Best Practices for computer Forensic Acquisitions.

unicef | para cada infancia