Derecho
Procesal Informático

PRUEBA DIGITAL

E-Mails, chats, SMS, WhatsApp, Facebook, filmaciones con teléfonos móviles, capturas de pantalla, contratos electrónicos, IA y otras tecnologías

Validez probatoria en el proceso civil, comercial, penal y laboral.

Dirección:
Horacio R. Granero

elDial.libros

Obtención e incorporación al proceso penal de pruebas de WhatsApp y otras aplicaciones

Por Maximiliano Hairabedián(*)

"Tanto los políticos como los votantes apenas pueden comprender las nuevas tecnologías, y no digamos ya regular su potencial explosivo. Desde la década de 1990, internet ha cambiado el mundo probablemente más que ningún otro factor, pero la revolución internáutica la han dirigido ingenieros más que partidos políticos".

Yuval N. Harari

I. Introducción

Son tantas las aplicaciones y usos que se le da al teléfono celular, que las llamadas son parte cada vez menos trascendentes.

(*) Doctor en Derecho y Ciencias Sociales (Universidad Nacional de Córdoba). Fiscal General Federal por concurso. Profesor Adjunto de Derecho Procesal Penal – Universidad Nacional de Córdoba. Profesor de post grado de Derecho Procesal Penal - Universidad Católica de Córdoba y Universidad Empresarial Siglo 21. Completó el Programa de Instrucción para Abogados (P.I.L.) en la Universidad de Harvard (Harvard Law School)

Los mensajes (*sms, WhatsApp, telegram*, correos electrónicos, etc.), las fotografías, videos, audios, localizaciones por GPS, búsquedas por la *web*, intereses, lecturas, archivos, notas, compras, operaciones bancarias, etc., pueden guardar los aspectos más íntimos de la persona. Hace un par de décadas las computadoras comenzaron a compartir espacios de almacenamiento de la intimidad con los lugares tradicionales (escritorios, armarios, bibliotecas, cajas, libretas, álbumes de fotos). Y más recientemente el mismo fenómeno ocurrió con los celulares. Tanta información obviamente constituye un reservorio importante de prueba, entre las que se destacan las aplicaciones de chats o mensajería.

Estos medios de comunicación no se agotan en las conversaciones de audio o escritas, sino que contienen mucha más información (intercambios de archivos, fotos, videos, ubicaciones) y sirven de puente para las más diversas actividades humanas (amistad, amor, odio, delitos, negocios, etc.). De allí el interés en escudriñar los problemas jurídicos cuando se pretende registrar un teléfono celular con fines de investigación penal.

Tomaré como muestra de análisis el programa más usado actualmente en Argentina, el WhatsApp, pero el desarrollo y las conclusiones de este trabajo pueden trasladarse a otras aplicaciones análogas (v.gr. Telegram).

II. Acceso al contenido de la mensajería

II.1 Requerimiento al proveedor del servicio

Hay distintas vías para obtener información de W*hatsApp* u otras aplicaciones. La más complicada, y por lo tanto menos utilizada en la práctica, es pidiéndoselo a la compañía, directamente o por medio de la cooperación judicial internacional[1]. El problema es que forma parte de lo que Marcos Salt[2] describe como "cooperación asimétrica" entre los Estados y las grandes empresas tecnológicas, que gozan de una relación de poder superior

[1] "Guía de buenas prácticas para obtener evidencia electrónica en el extranjero", UFECI, MPF, 2020.

[2] Salt, Marcos, "La ciberdelincuencia y el acceso a la evidencia digital", HDI, Podcast, 11/11/2020.

por ser las dueñas de los datos[3] y las que fijan las reglas para su entrega[4].

Además, si lo que se quiere obtener son las conversaciones y archivos intercambiados, lo más probable será toparse con la pared de la dificultad técnica[5]. Podrá advertirse que las chances

---

[3] "Quienes poseen los datos poseen el futuro", dice Harari en 21 Lecciones para el Siglo XXI.

[4] *WhatsApp* anuncia: "Únicamente revelamos datos de las cuentas de nuestros usuarios de acuerdo con nuestras condiciones de servicio y la legislación aplicable. Adicionalmente, evaluaremos si las solicitudes se apegan a estándares internacionalmente reconocidos, tales como los derechos humanos, el debido proceso y el estado de derecho. Para exigir la revelación del contenido de una cuenta, es posible que se deba presentar una solicitud de asistencia judicial mutua o un exhorto" (Información oficial para fuerzas del orden en procesos internacionales, https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities/?lang=es.). Si se trata de procesos tramitados bajo la ley norteamericana, la compañía advierte que sólo revela "datos de las cuentas de acuerdo con nuestras condiciones del servicio y la legislación aplicable, incluida la ley federal estadounidense de almacenamiento de datos ("Stored Communications Act", SCA), 18 USC, secciones 2701-2712", pasando a especificar los requisitos impuestos por la legislación estadounidense (oficio emitido en investigación criminal para exigir la revelación de datos básicos del suscriptor -nombre, fechas del servicio, direcciones IP, correo electrónico-; u orden de un tribunal basada en causa probable para el contenido). Aclara que "durante la prestación normal de nuestros servicios, WhatsApp no guarda mensajes una vez han sido entregados ni registros de transacción de esos mensajes entregados, y los mensajes no entregados son eliminados de nuestros servidores pasados 30 días. WhatsApp cuenta con cifrado de extremo a extremo para nuestros servicios, el cual está activo siempre".

[5] El cifrado *end-to-end*, implica que ni siquiera el prestador del servicio puede acceder al contenido cifrado, por lo tanto, aunque a través de una carta rogatoria (que ya es complicado) consiguiéramos requerir a WhatsApp que nos facilitara el contenido de una conversación entre usuarios suyos, esta compañía, a día de hoy, debería respondernos que no le es posible, ya que "no resguarda ningún tipo de registro sobre aquellos mensajes generados a través de su plataforma, y adelantamos que esta característica revestirá gran importancia al tratar los medios de prueba en especial" (Bielli, Gastón E., "**Los mensajes de WhatsApp y su acreditación en el proceso civil", La Ley, 29/10/2018, p. 1). Se ha señalado que por esta característica, diferente a otras redes sociales que almacenan el contenido, l**a única información que pueden facilitar los proveedores es la que se denomina metadatos, definidos como datos sobre datos o la información generada por los usuarios cuando utilizan tecnologías digitales (Pérez Astudillo, N., "Los medios telemáticos como prueba de cargo en el proceso", *Cuadernos Digitales de Formación nº 3, 2015,* Consejo General del Poder Judicial, p. 8), tales como la constatación del tráfico de las comunica-

de tener éxito por esta vía son bajas, más aún si se trata de la investigación de un delito común y corriente. Entonces, las formas usuales de acceder al contenido, son otras.

II.2 Aporte del usuario

El aporte voluntario de la víctima o testigos de sus comunicaciones por *WhatsApp*, no presenta mayores conflictos constitucionales (p. ej., una persona denuncia que lo están amenazando por *WhatsApp* y pone a disposición su móvil para constatarlo). Desde el punto de visto de la protección de los derechos constitucionales no es necesaria ninguna autorización judicial específica, toda vez que, quien es parte de la comunicación, da su consentimiento para la injerencia, siendo irrelevante que afecte a otro porque no existe un deber jurídico de guardar reserva de las propias comunicaciones

II.3 Adquisición coercitiva mediante registro y requisa

Cuando se trata de la obtención coercitiva del celular donde está instalado *WhatsApp*, hay que diferenciar distintas situaciones. Si el aparato está dentro de un domicilio, hará falta orden de allanamiento para su incautación, como con cualquier objeto que pueda servir de prueba. La autorización judicial genérica de registro no habilita a revisar los mensajes, imágenes, etc., sin orden expresa, urgencia o necesidad[6].

---

ciones, origen y destino de las mismas, datos conservados sobre identidades y nombres de usuario y claves, incluidos el número de abonado telefónico asociado o la IP de referencia, sin perjuicio de la posibilidad de interceptación futura a través de la correspondiente autorización judicial, pero el acceso a contenidos ya emitidos no resulta posible si se acude al administrador de la aplicación (Betrán Pardo, Ana Isabel, "Los contenidos de WhatsApp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer", 30/9/2015, http://www.pensamientopenal.com.ar/system/files/2015/10/doctrina42246.pdf).

[6] Con un criterio más amplio, el Tribunal Supremo español ha convalidado inspecciones de mensajes durante el allanamiento, fundándolo en que la interferencia de la policía en la comunicación del coacusado en su teléfono móvil, se produjo una vez consumado el proceso comunicativo del mensaje y de que el destinatario de éste hubiera tomado conocimiento de su contenido, por lo que la injerencia posterior podrá afectar en el derecho a la intimidad pero no el secreto de las comunicaciones invocado por el recurrente. "En estas circunstancias (orden judicial y secuestro de pastillas de MDMA), la lectura del mensaje grabado se encuentra bajo la cobertura de la autorización judicial como si de

Si el equipo telefónico es trasladado o tenido por una persona en la vía pública o en un lugar de acceso al público, serán de aplicación las disposiciones sobre requisa personal para su incautación: la policía podrá secuestrarlo sin orden judicial cuando se trate de un acto urgente o impostergable fundado en sospecha de la comisión de delito; y si no hubiere urgencia deberá procederse con orden de juez (CPPN., 184 inc. 5°, 230 y 230 bis), o del fiscal en los sistemas acusatorios que así lo habilitan (CPPCba., 208).

Lo importante es que tanto el procedimiento de adquisición del teléfono celular como el de su revisación se hayan realizado sin infringir derechos y garantías constitucionales, de lo contrario serán de aplicación las exclusiones probatorias y la ineficacia se extenderá al proceso de adquisición de los datos (p. ej., si secuestraron el móvil en un allanamiento sin orden), salvo que medien excepciones a la doctrina de los frutos del árbol venenoso[7].

---

otro papel o documento se tratara que pudiera relacionarse con el tráfico de las drogas incautadas cuya intervención y "objetos de cualquier tipo relacionados con ellas" constituía el objeto de la diligencia de entrada y registro"; excluida la vulneración del secreto de las comunicaciones, tampoco ha sufrido lesión el derecho a la intimidad porque la Policía hubiera invadido el ámbito de la privacidad al leer la misiva grabada en el móvil, y ello no sólo por la autorización judicial que ampara esa actuación, ya analizada, sino también porque el examen del tan repetido mensaje se revela como una acción prudente, razonable y proporcionada, atendidas las circunstancias, como una excepción a la regla general de la necesidad de mandato judicial para invadir la esfera de la intimidad de la persona" (STS., 1235 del 27/6/2002).

[7] Hairabedián, Maximiliano, Eficacia de la prueba ilícita y sus derivadas en el proceso penal, Editorial Ad Hoc, 2° edición, 1° reimpresión, Buenos Aires, 2016. Un caso que ilustra esta situación fue el de una persona que olvidó su celular en un comercio. El comerciante que lo encontró revisó su contenido, descubriendo videos en los que aparecía el abuso sexual a un niño. Radicada la denuncia se desencadenó una investigación, en la que se determinó el autor del aberrante hecho. El fallo que convalidó el procedimiento judicial, reconoció que la protección del artículo 18 de la CN a la correspondencia y papeles privados comprende también a los correos electrónicos, llamados telefónicos o mensajes de texto porque tiene por finalidad garantizar el respeto a la vida privada de la persona en sus ámbitos más íntimos, "por lo que resulta difícil excluir a los registros audiovisuales que un individuo conserva en su computadora personal, sea en una memoria de almacenamiento (pendrive) o, como en este supuesto, en un teléfono móvil". Pero se consideró que el olvido del titular en un lugar de acceso público, la buena fe del que lo encontró y la gravedad del descubrimiento ameritaban la validez probatoria (CNACC., Sala de Feria A, 16/1/2016, "C.Q., A.G. s/nulidad", L.L., Suplemento Penal, junio 2015, ps. 29 y ss.).

Esta cuestión ha sido objeto de pronunciamiento por la Corte Suprema de Estados Unidos, que se pronunció en contra de la revisión policial de celulares sin orden judicial[8]. Se trató de un caso en que la policía interceptó un vehículo que tenía las placas vencidas y el conductor suspendida la licencia. Cuando hacían el inventario de los efectos del vehículo encontraron dos armas de fuego. Al ingresar detenido al conductor en la comisaría, le retuvieron un *smartphone* que llevaba en su bolsillo. Como estaban investigando resonantes hechos violentos vinculados a pandillas y los policías sospecharon que el arrestado podía estar involucrado, le revisaron los mensajes, observando que se vinculaban con el argot y la actividad de una de las bandas. Por ello le pasaron el teléfono móvil a policías abocados a la investigación de las pandillas y al registrar los datos del equipo encontraron fotos y videos que incriminaban al detenido. Tras los planteos defensivos, la Corte de aquel país resaltó que, aunque los detenidos tienen disminuido su derecho a la privacidad, esto no significa que lo pierdan totalmente, ya que no toda injerencia está permitida. Reconoce que los datos digitales que contienen los celulares tienen trascendencia constitucional porque se han transformado en una parte esencial e importante de la vida cotidiana, al punto que "un visitante proverbial de Marte podría concluir que eran una característica importante de la anatomía humana". Destacaron los jueces que estos teléfonos se diferencian tanto en sentido cuantitativo como cualitativo de otros objetos que puedan estar en poder de una persona detenida, porque el término 'teléfono celular' es en sí mismo engañoso; muchos de estos dispositivos son en rigor minicomputadoras que también tienen la capacidad de ser utilizados como un teléfono; podrían ser fácilmente llamados cámaras, reproductores de video, calendarios, grabadoras, bibliotecas, diarios personales, álbumes, televisores, mapas o periódicos. Sin embargo, observa Carral, pareciera que la Corte está dispuesta a dejar abierta la posibilidad para que en "casos extremos" se pueda proceder de urgencia, y al respecto señala: si "la policía está

[8] "Riley vs. California", 573 U.S. 132, 25/6/2014 (también se expidió en igual sentido en "US vs. Wurie", 573 U.S. 212). Para la exposición del caso y los fundamentos seguimos el comentario y traducción de Carral, Daniel, "¿Smartphones con garantía extendida?", Revista de Derecho Penal y Procesal Penal Abeledo Perrot N° 7, 2015, ps. 1404 y ss.

verdaderamente enfrentando una situación de 'ahora o nunca' —por ejemplo, ante circunstancias que sugieren que el teléfono de un acusado será objeto de un control remoto inminente que destruirá la información—, los oficiales de policía están habilitados a confiar en esas circunstancias extremas para registrar el teléfono inmediatamente"[9]. La Corte resaltó la necesidad de autorización judicial porque "la capacidad de almacenamiento de los teléfonos celulares tiene varias consecuencias relacionadas con la vida privada" por todos los tipos de informaciones que almacena: "La suma de la vida privada de un individuo puede ser reconstruida a través de un millar de fotografías etiquetadas con fechas, lugares y descripciones; lo mismo no puede decirse de una o dos fotografías de sus seres queridos guardados en una cartera".

En el ámbito nacional, el artículo 151 del nuevo Código Procesal Penal Federal, al regular el régimen legal de la incautación de datos, acota la discusión exigiendo orden judicial para la revisación de los equipos cuando son secuestrados por la policía. De todas formas, la discusión no está saldada, porque ese Código aún no está totalmente implementado y, por otra parte, en las jurisdicciones provinciales hay jurisprudencias dispares[10].

---

[9] En la misma línea se ha pronunciado la reforma a la ley de enjuiciamiento española, que prevé que la policía puede hacer un examen directo de los datos del dispositivo incautado en aquellos casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado (art. 588 sexies c). El protocolo de manejo de evidencia digital elaborado por el Ministerio Público Fiscal argentino (Res. PGN N° 756, 31/3/2016) establece que salvo situaciones de emergencia que lo ameriten, los celulares y otros elementos "no deben ser operados, y por ende, deben ser resguardados de forma inmediata", previéndose que "si las circunstancias del caso hacen necesario que se deba acceder a los datos o información contenida en las computadoras o dispositivos de almacenamiento informático, la persona que efectúe dicha tarea debe ser idónea, es decir, contar con los conocimientos técnicos informáticos que la situación merece y, a su vez, capaz de explicar el motivo por el cual debió interactuar con la evidencia digital -por lo general, la urgencia del caso-, y los pasos llevados a cabo".

[10] A favor de la revisión policial sin orden, TSJCba., Sents. N° 135, 21/5/2010, "Benítez" y N° 417, 31/10/2014 en "Flores" –fallos en los que prácticamente se equipara el celular a cualquier cosa objeto de inspección ocular-; en contra TCasPenBA., Sala I, Reg. 119, 1/3/2015, "R., V.".

En relación a la posibilidad de acceder al *WhatsApp* de manera remota mediante la instalación de un *spyware* en el celular del investigado, no obstante, la falta de regulación legal específica[11], será posible hacerlo con la orden fundada del juez, ya que encuentra amparo en las disposiciones procesales sobre intervención de comunicaciones. Desde el punto de vista constitucional no hay una diferencia cualitativa y sustancial entre la intervención de comunicaciones hecha por el método tradicional y la realizada mediante un programa espía porque los recaudos no varían (orden jurisdiccional, fundada, limitada en el tiempo, determinada, proporcionada) y la materia u objeto de conocimiento generalmente es la misma (las comunicaciones del investigado)[12].

III. Incorporación del contenido

El contenido del W*hatsApp* (mensajes escritos, audios, fotos, videos) forma parte del concepto moderno de prueba documental, que no se agota en el clásico instrumento escrito en papel, sino que abarca también las expresiones contenidas en soportes digitales[13].

Una vez que se ha accedido legalmente al contenido del celular, sea por orden del juez en casos de secuestros durante alla-

[11] El art. 151 del nuevo Código Procesal Penal Federal regula la incautación de datos, pero está discutido su alcance remoto. Salt interpreta que no incluye los datos alojados en un sistema informático distinto pero conectado al sistema original y menos aún que habilite la obtención extraterritorial (Salt, Marcos, Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remotos a datos digitales, Ad Hoc, Buenos Aires, 2017, p. 307). En otra visión, hemos interpretado que la norma abarca los datos alojados en servidores, nubes o discos duros externos (Hairabedián, Maximiliano, Código Procesal Penal Federal comentado, Ad Hoc, 2021, p. 328).

[12] Sobre los principales reparos, respuestas y legislación comparada sobre la cuestión, puede verse Hairabedián, Maximiliano, Investigación y prueba del narcotráfico, Ad Hoc, Buenos Aires, 2020, ps. 331 y ss.

[13] CP., 77; Cód. Civil y Com., 284 y ss. "Comprende todo escrito no firmado, entre otros, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información" (art. 287). "Representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo" (art. 6 ley 25.506).

namientos o requisas, o por presentación o exhibición voluntaria del poseedor, la información útil y pertinente deberá ser introducida al proceso.

En cuanto a la forma, rige la libertad probatoria (documental –v. gr. impresión, acta de constatación, captura de pantalla, etc.-; constancia en declaración testimonial, etc.), pudiendo escogerse la vía procesal que resulte más adecuada[14].

Si la impresión de pantalla es ofrecida por un particular, deberá ser constatada su correspondencia con el contenido original obrante en el celular, lo que puede ser certificado por un funcionario público (p. ej., sumariante o secretario judicial que tiene los elementos a la vista) desde el inicio mismo del proceso[15] (v.gr. en el momento de la denuncia), o por un escribano[16] antes o durante la sustanciación del procedimiento penal.

---

[14] Los archivos de texto, audio, fotos, vídeos podrán tener acceso al proceso como prueba documental (pública o privada, según sea el caso), pericial, reconocimiento o inspección personal, interrogatorio del acusado o los testigos, instrucción en un soporte determinado que pueda ser reproducido en el juicio oral, como puede ser el papel, (Betrán Pardo, ob. cit). También puede consultarse, Rodríguez Lainz, J.L.," Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea", *La Ley España, N° 8569,* 25/6/2015).

[15] En materia comercial se consideró que "la constatación judicial de distintas capturas de pantalla del celular del hijo del actor, como así también el oficio a Mercado Libre S.R.L y la constatación por parte del personal del juzgado en la sede de venta de la concesionaria –para verificar si el vehículo sigue, o no, ofrecido en venta-, son medidas que el recurrente pudo haber intentado concretar extrajudicialmente a fin de consolidar la posición que esgrime en su favor" y que "el aseguramiento de pruebas en los términos del art. 326 del CPCC, constituye una vía procesal de excepción, que sólo debe admitirse si se comprueba que el proponente se halla expuesto a perder la probanza o que la misma le resultará imposible o de muy difícil realización en una ulterior oportunidad" (CNCom., Sala A, 21/10/2020,"Alhadeef c/ Trepat Automóviles SA s/ medida precautoria", elDial.com - AAC56E).

[16] Se han señalado las actas ante escribano público como medio idóneo para incorporar "prueba electrónica, como son los mensajes por WhatsApp, al proceso como instrumental, siempre y cuando la misma se confeccione correctamente… como regla general, el fedatario procederá a transcribir esos mensajes a la correspondiente acta, indicando la existencia de los mismos, las fechas y horarios del intercambio, contenido de los mensajes, desde que número de teléfono se remitieron, el modelo del dispositivo, su código de fabricación, marca, IMEI, identidad presunta de a quien fue dirigido el intercambio, entre otras cuestiones que podrá verificar a través de lo que se logra "visualizar" (Bielli, Gastón, ob. cit.).

Si la impresión de pantalla carece por completo de certificación, su fuerza convictiva se reduce considerablemente por lo que, aisladamente y sin otros elementos que corroboren su autenticidad, difícilmente pueda dar base a una condena fundada, y menos aún si ha sido controvertido su contenido[17].

La cantidad de detalles útiles que tenga el acta o la información en ella verificada, aumentará su calidad probatoria y contribuirá a prevenir o neutralizar eventuales cuestionamientos que puedan hacerse a posteriori. Por ejemplo, desde los más comunes (fecha, hora, remitente, destinatario y contenido) hasta la impresión o descripción de los *emojis* que integran la comunicación (dado su enorme valor expresivo), confirmaciones de lectura (p. ej., los doble tildes azules), el número de teléfono asociado al contacto en la agenda (p. ej., si el mensaje aparece en pantalla enviado por "Pepe", sería conveniente que se deje constancia de que línea le corresponde[18]). También si se trata de un chat

[17] "En relación a la prueba de "capturas de pantallas" aportadas en la presente causa, al no tener metadatos y poder ser fácilmente alteradas, no son prueba electrónica, pero constituyen prueba indiciaria, cuya valoración corresponde analizarla en conjunto con los demás elementos probatorios del caso"; "el ingreso al expediente judicial de meras capturas de pantalla es la metodología más utilizada por los letrados, a fin de demostrar la ocurrencia de hechos que se canalizan vía plataformas de mensajería instantánea. Estos «pantallazos», en la mayoría de los casos, son impresos por la parte y aportados al expediente como prueba documental, sin intervención de un fedatario público". "Cuando se trata de hechos que ocurren dentro del núcleo íntimo, por tratarse de relaciones muy cercanas, es posible que dichos hechos sean difíciles de demostrar. Es así que este principio está consagrado en el art. 16 inc. i de la Ley 26.485, es decir, que se flexibilizan las reglas aplicables para la admisión y valoración de las pruebas, permitiéndose al juez la admisión del elemento probatorio, como una forma de subsanar los problemas que pueden suscitarse al invocar y demostrar cualquier hecho relacionado con el marco de violencia de género" (CamCrim. Correc., 3ª, La Rioja, 7/6/2021, "Pioli"). En un proceso laboral se consideró que los mensajes de *WhatsApp* no resultan "una prueba confiable sin la certificación o pericia técnica que los avale, toda vez que puede resultar fácilmente alterado el remitente de los mensajes, por lo que no resulta prueba contundente sobre los supuestos encargos de trabajo ni sobre la modalidad de la supuesta relación laboral que pretende la actora" (SCMendoza, 14/12/2020, "Bastias c/ Freire-despido", elDial.com - AAC530).

[18] En la extracción de información de celulares secuestrados, es prácticamente de rutina el volcado del contenido de la agenda de contactos, lo que permite luego unir a los remitentes y destinatarios de las comunicaciones. Este aspecto suele resultar de utilidad en el análisis de la prueba de cargo. Así, se ha va-

exportado desde la aplicación (p. ej., enviado o copiado previamente desde *WhatsApp*), resultará útil constatar su correspondencia con la aplicación.

IV. Valoración

El extensivo uso de *WhatsApp* y otras redes sociales presenta el interés de su uso con fines probatorios. Su contenido puede ser útil y pertinente para probar diversos aspectos del objeto de prueba: a veces será la materialidad o manifestación misma del delito, como sucede en aquellos en que la conducta típica se realiza mediante el discurso o la comunicación (p. ej., amenazas, extorsiones, organización del narcotráfico, compraventa de bienes ilícitos, difusión o tenencia de pornografía infantil, pornovenganza, etc.). En otros casos servirá como evidencia relevante para reconstruir lo sucedido (p. ej., la exhibición del objeto robado, el arma utilizada o el relato del hecho), por sí o de manera complementaria a otras evidencias[19]. También como prueba de contexto (p. ej., violencia de género) o para acreditar el dolo o desvirtuar la posición exculpatoria[20], e inclusive para cuestiones

---

lorado para fundar la condena la "conversación de interés que mantuvo con el abonado nº 1169168840 contacto agendado como… como así también la foto del comprobante de la encomienda que diera origen a esta investigación" (CFCP., Sala IV, Reg. 997, 2/7/2021, "Zárate Jara").

[19] "Comunicaciones receptadas en los aparatos incautados revelaron actividades contemporáneamente desarrollaban por los titulares involucrados, vinculadas con conductas compatibles con el negocio minorista de estupefacientes. Esas breves manifestaciones entre los interlocutores, extraídas de mensajes y diálogos interceptados, que en principio parecerían referirse al acontecer cotidiano, conjugados a los movimientos en el domicilio registrados en los videos (que fueron exhibidos en el debate) y que se corroboraron en los testimonios indicados permitieron determinar que responden a actividades compatibles con la venta de tóxicos prohibidos, los que se encontraron posteriormente en sus viviendas al ser allanadas" (CFCP., Sala III, Reg. 1213, 14/7/2021, "Herrera").

[20] La casación federal respaldó la valoración incriminatoria de una sentencia condenatoria basada en que "resultan esclarecedores los mensajes encontrados en el celular secuestrado", ya que, "aún sin ser prueba dirimente, son elocuentes en cuanto al conocimiento que tuvo sobre la droga transportada y el medio utilizado para ello", en razón de que "la exploración del artefacto permitió constatar la existencia de numerosos intercambios de mensajes a través de la aplicación "WhatsApp" que permiten recrear un panorama muy distinto al

procesales (v.gr. validez de prueba, nulidad de procedimientos, notificaciones)[21].

Como todo elemento de prueba, la valoración de la mensajería en un proceso está supeditada a las reglas de la sana crítica racional. La experiencia indica que, en general, los documentos obtenidos de los servicios de mensajería son reales, sean conseguidos por organismos técnicos desde el celular secuestrado, o aportados por particulares. En el primer caso la presunción de veracidad es mayor, por la fe pública de la que gozan los procedimientos oficiales; en el segundo –aporte de particulares- se

---

presentado en su declaración por el justiciable, donde dio a entender que era víctima de su empleador", concluyendo que " el tenor de las comunicaciones analizadas no deja margen de duda en cuanto a la habitualidad y voluntariedad con la cual se dedicaba al comercio de sustancias estupefacientes, actividad que no se circunscribía únicamente a cumplir con el envío de los pedidos, como insinuara el mentado en su declaración" (CFCP., Sala III, Reg. 771, 2/6/2021, "Dos Santos").

[21] La jurisprudencia convalidó la validez de un procedimiento coordinado y trasmitido por *WhatsApp*. El tribunal de juicio lo avaló señalando: "sin perjuicio de no saberse el momento preciso en que el secretario puso el cargo, lo que sí se pudo establecerse es que a la orden la pidieron los preventores, sin que hubiera una actividad autónoma del juez", derivada "de los acontecimientos en los que se lo participaba por WhatsApp. "Era un día domingo, donde tanto policías como funcionarios judiciales y gendarmes fueron convocados de manera no planificada, por la urgencia de los acontecimientos y por la velocidad con la que éstos se desarrollaban, y que, dada la prórroga de jurisdicción, se activaron notificaciones por medios informales que luego se documentaron en soporte papel" y "dentro de la vorágine de ese momento no tuvo (la orden de allanamiento) el circuito que normalmente tiene en un día hábil". "En la criminalidad ligada a la ley de estupefacientes la volatibilidad de la prueba autoriza y legitima una dinámica de actuación a una velocidad diferente a aquella que alguna vez imaginaron los teóricos que originaron el proceso penal mixto". "Tanto los efectivos de Gendarmería Nacional, como el personal de la División Precursores Químicos de la Policía Federal Argentina, conformaron un grupo de WhatsApp, del que también participaron integrantes del Juzgado Federal nro. 1 de Salta, siendo este "el único modo posible de vinculación de las fuerzas de prevención con la jurisdicción", a la luz de las particulares características de esta causa, "donde el equipo de investigación se conformaba con dos fuerzas distintas, la jurisdicción actuaba en prórroga de jurisdicción…a 1600 kilómetros de Salta". Y la alzada confirmó lo decidido por el tribunal que impuso la condena: "el planteo nulificante reeditado por las defensas resulta infundado, con el solo objeto de hacer caer todo el juicio, a pesar de que no media inobservancia de ninguna disposición que conlleve el dictado de la pretensa nulidad, toda vez que no fue verificada violación a garantía alguna ni la comisión de perjuicio cierto e irreparable" (CFCP., Sala III, Reg. 1095, 7/7/2021, "Abdala").

puede ver reducida la credibilidad, sobre todo cuando es controvertida. En este último supuesto, su valor dependerá de las restantes pruebas que permitan confirmar o desvirtuar el contenido del *WhatsApp* puesto en crisis[22].

La posibilidad de manipular, alterar o falsificar este tipo de prueba es una realidad. Los mensajes pueden borrarse total o parcialmente modificando el contexto de la conversación, existen mecanismos que permiten crear *ex novo* mensajes de texto, editar los recibidos o simular el envío y recepción, manipulando incluso su hora[23].

---

[22] En esta línea, el Tribunal Supremo español confirmó la validez de la transcripción de los diálogos mantenidos por una menor con un amigo a través de la red social Tuenti, a quien le contó los abusos sexuales por parte del novio de su madre. Puntualizó que estas pruebas deben abordarse con "todas las cautelas", debido a que "la posibilidad de una manipulación forma parte de la realidad de las cosas", ya que "el anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo". Entonces, si las conversaciones se ponen en duda, cuando se aportan a la causa archivos impresos, se desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria, siendo indispensable realizar una prueba pericial para identificar el verdadero origen de esa comunicación, la identidad de sus interlocutores y la integridad de sus contenidos (STS 2047, Sala Penal, 19/5/2915). El Tribunal confirmó la condena rechazando la alegación de manipulación, porque la víctima puso a disposición del juez su contraseña de Tuenti para que, si se cuestionaba, se comprobara su autenticidad mediante un informe pericial. También valoró que el amigo de la víctima declaró como testigo en el juicio donde pudo ser interrogado por las acusaciones y las defensas. En comentario a este criterio, se ha señalado que "no es posible entender cómo se deduce del recurso que estas resoluciones establezcan una presunción iuris tantum de falsedad de estas modalidades de mensajería, que debe ser destruida mediante prueba pericial que ratifique su autenticidad y que se debe practicar en todo caso; sino que, en el caso de una impugnación (no meramente retórica y en términos generales) de su autenticidad -por la existencia de sospechas o indicios de manipulación-, se debe realizar tal peritaje acerca del verdadero emisor de los mensajes y su contenido…medida (que) no será precisa cuando no exista duda al respecto mediante la valoración de otros elementos de la causa o la práctica de otros medios de prueba" (Altamira, Matías, Introducción del WhatsApp en el proceso penal", Comercio y Justicia, Córdoba, 15/4/2019).

[23] Betrán Pardo, ob. cit. relata que la Asociación de Internautas publicó en agosto de 2014 distintos modos de crear y modificar mensajes de *WhatsApp* sin la necesidad de grandes conocimientos. También sitúa en un nivel básico de intrusión la manipulación de una red local wi-fi; o asignar un nombre de usuario a la persona que se quiere dañar, simular el envío de mensajes y a partir de allí aportar al proceso un documento impreso con la captura de pantalla que

Aunque en la mayoría de los casos no ocurre, si se presenta un planteo fundado en tal sentido, que no puede ser esclarecido con las demás pruebas del proceso, la pericia informática será el medio idóneo para despejar la duda[24].

Los métodos para obtener las conclusiones periciales son de incumbencia del experto que practicará esa prueba y pueden variar a medida que avanza la ciencia de la informática forense. Se han descripto dos metodologías de obtención de estos datos electrónicos sobre los dispositivos: la primera, "un proceso de borrado, descarga y reinstalación de la aplicación, forzando a que se produzca la restauración de los datos que WhatsApp guarda en la nube, lo que consecuentemente importara los mensajes que son "backupeados" a diario por la plataforma (generalmente en una cuenta de Google Drive)". La segunda es el "volcado forense de memoria", procedimiento más complejo dirigido "a

---

contenga el mensaje o archivo correspondiente, alegando la pérdida, borrado o destrucción del mensaje o incluso del propio terminal telefónico. Después de mencionar sistemas más sofisticados, ilustra la autora que cuando se hayan empleado programas espía u otras modalidades de software malicioso que permitirán la emisión de mensajes desde el propio terminal usurpado o aprovechando la información obtenida sobre clave de seguridad, nombre de usuario y clave de acceso, etc., la solución parte de un examen exhaustivo de la memoria interna del terminal. La investigación pericial se centrará en verificar en el volcado de la memoria, de los códigos propios de estos programas; localizar la dirección IP del servidor al que reenvía los datos en su caso; localizar el número de abonado teléfono oculto con el que se conecta para reenviarle la información, y en los archivos temporales localizar la datación de la instalación del programa.

[24] "En Google "Play Store" tenemos a nuestro alcance (y de forma gratuita) aplicaciones como "WHATSFAKE" o "FAKE CHAT". Estas App permiten sustituir o suplantar una conversación real de WhatsApp. A pesar que su intención es entretener y divertir, lo cierto es que consiguen hacer cosas increíbles como modificar la hora de envío, el estado de recepción, el emisor del mensaje, enviar audios, vídeos y fotos que pueden ser configurados como los mensajes. Además, permiten cambiar los ajustes de los perfiles y estados de las personas implicadas tal y como aparece en las conversaciones de WhatsApp reales. Un pantallazo, es una imagen que cualquiera podría modificar con Photoshop o cualquier otro programa de edición de imágenes". Para detectar una manipulación de WhatsApp como prueba en juicio está el perito informático, que "dispone de los conocimientos y herramientas para extraer las conversaciones originales de la APP, así como para certificar y mantener la cadena de custodia de las mismas" (Picón Rodríguez, Eugenio, "¿Por qué no es válida una conversación de WhatsApp en juicio?", https://elderecho.com/por-que-no-es-valida-una-conversacion-de-whatsapp-en-juicio).

un análisis de los archivos insertos en el dispositivo" para el que es necesario "efectuar copias forenses exactas de la información acumulada, certificadas a través de un código alfanumérico de dicha información (el denominado hash, que vendría a ser el ADN del archivo o conjunto de estos)" y tras distintos pasos de validación hash, "si los códigos coinciden, se puede aseverar que la prueba electrónica analizada se mantuvo inalterada"[25].

Otra vía respaldatoria puede ser la prueba informativa, dirigida a los organismos o empresas que registran las titularidades de los titulares de teléfonos celulares[26]; o también a la empresa que maneja la aplicación, para que confirme la existencia de las comunicaciones o intercambios, pero en este último supuesto las dificultades prácticas lo desaconsejan[27].

---

[25] Bielli, Gastón E., ob. cit. El autor señala que, respecto a los puntos de pericia, se podrían solicitar algunos de los siguientes, relacionados al celular que aporta la parte: línea se encuentra vinculado el dispositivo; IMEI; determinar si la cuenta de WhatsApp inserta en ese dispositivo se encuentra vinculada a la línea telefónica XXXX; determinar si con fecha XXX se produjo un intercambio de mensajes a través de WhatsApp entre el móvil número XXX y el móvil número XXX; transcribir el contenido de los mensajes intercambiados estableciendo los horarios exactos en que se produjeron y diferenciando cuales fueron emitidos y recepcionados por esta parte y por la contraria; determinar la integridad de los mensajes intercambiados; establecer específicamente que mensajes fueron efectivamente visualizados (mediante el "tilde azul") por la parte contraria.

[26] La casación federal convalidó la condena por siembra, cultivo y comercio de estupefacientes, valorando, entre otras pruebas, "las capturas de la aplicación "WhatsApp", específicamente en cuanto al numeral del abonado telefónico, complementado con las consultas informáticas del sitio "Enacom"" (CFCP, Sala unipersonal, Reg. 908, 3/6/2021, "Machado, Germán Leonel s/recurso de casación").

[27] Por medio de este requerimiento, decretado a solicitud de parte, se procurará que WhatsApp Inc. emita un informe circunstanciado mediante el cual se establezcan los antecedentes existentes en sus servidores acerca de un intercambio de mensajes establecido entre dos cuentas de usuario. Es así que se procurará lograr la intervención de la plataforma de mensajes como tercero que certifique el contenido de la conversación invocada, con el objeto de incorporar dicho informe como prueba en el pleito judicial.
"La aplicación WhatsApp pertenece a Facebook Inc. desde el año 2014, subsidiaria de Facebook, pero independiente legalmente"; el sistema de pedidos por rogatoria internacional es un trámite complicado vía cancillería, y aun así "la aplicación no tendrá acceso (a contenido), si se lo piden las autoridades y en su nota oficial afirma(rán) que no mantienen registro de los mensajes en sus propios servidores y que el fin del cifrado de extremo a extremo se busca protegerlo "manos indebidas»" (Bielli, Gastón E., ob. cit.).

V. Recuperación de datos eliminados

La eliminación de información de los celulares es tan natural como el constante descarte de objetos que nos rodean. Así como tiramos elementos físicos a la basura, también lo hacemos con los digitales. Las finalidades pueden ser muchas: limpieza, orden, prevención o exceso de acumulación, protección de la privacidad, destrucción de pruebas comprometedoras, etc.

Por eso en la investigación penal puede ser útil la búsqueda en la basura. Si se trata de los residuos clásicos, tradicionalmente se ha justificado la práctica policial sin orden judicial, en que la persona se ha desprendido de los elementos descartados sin intención de seguir sometiéndolos a su dominio, quedando así expuestos a la apropiación. Ahora bien, cuando hablamos de basura informática la cosa cambia. Aquí la porción de privacidad contenida puede ser mayor. Los objetos físicos que arrojamos al tacho, si un policía no lo recogió rápidamente, en horas lo será por un camión y terminarán en algún enterramiento o centro de reciclaje mezclados, perdidos y confundidos con miles de toneladas de desperdicios. En cambio, los archivos, fotos, mensajes, mails, audios, que eliminamos pueden seguir almacenados por mucho tiempo en nuestro equipo, aun cuando muchas personas no lo sepan y crean que con apretar "suprimir" lo han borrado de la existencia. Cuando se eliminan datos de una computadora o celular, el sistema lo manda a un sector donde no queda directamente visible el acceso, algo que sucede inclusive con el borrado de conversaciones mantenidas por sistemas de mensajería como el popular *WhatsApp*[28].

[28] La principal peculiaridad de la aplicación *WhatsApp* y lo que a la vez constituye un gran obstáculo para verificar su autenticidad e integridad en el marco de un procedimiento judicial, es que la información transmitida no es conservada en un servidor externo perteneciente al administrador y sólo se conserva en el dispositivo de quienes se comunican, de forma que si todos o alguno de los comunicantes borra total o parcialmente el contenido de una conversación, la misma desaparece del terminal, quedando almacenados en segundo plano en la memoria flash donde se mantiene hasta el momento en que la necesidad de espacio en la memoria implica su eliminación, pues se solapan unos datos encima de otros. Por eso "la única forma de acreditar la existencia de estos contenidos es a través de los teléfonos móviles que han intervenido como emisor y receptor. No se guardan, pues, en la tarjeta SIM, sino en la memoria interna del aparato o en la tarjeta de memoria tipo SD, la cual, si es trasladada a otro

La recuperación del contenido eliminado es importante, no sólo por lo que se puede conocer a partir de su descubrimiento, sino también porque denota la intención de ocultarlo. El mero hecho de borrar elementos no significa nada, de hecho, es una actividad que todos hacen en su vida digital y en la inmensa mayoría de los casos no tiene que ver con motivaciones ilícitas (p. ej., la liberación de espacio para memoria es muy frecuente). Pero cuando se logran reflotar mensajes, fotos y videos incriminantes, la cosa cambia[29].

El medio probatorio para recuperar información borrada de un celular debería ser la pericia, porque requiere la intervención de un experto que, mediante herramientas de informática forense para acceder, descubra el elemento probatorio reflotando o recuperando los datos eliminados. La consecuencia práctica de esta conclusión debería conducir a que las partes puedan ejercer el derecho a controlar las operaciones técnicas mediante peritos particulares.

Sin embargo, es discutible la naturaleza conclusiva de este procedimiento, lo que ha permitido que en la práctica se le suela dar el mismo trámite de la inspección del celular para extracción del contenido no borrado. Al ser esta última una operación de carácter descriptiva generalmente factible de reproducción, no encuadra dentro de las pericias y no se notifica previamente. Por eso, la jurisprudencia ha sostenido que es válida la extracción de datos de un sistema informático mediante la utilización de un *software* específico sin intervención de la defensa, porque no es una pericia y por lo tanto no requiere notificación previa, toda vez que el artículo 233 del CPPN autoriza al juez a ordenar la obtención de copias o reproducciones de las cosas secuestradas, y el art. 151 del nuevo Código Federal regula el registro de un sistema informático o de un medio de almacenamiento de da-

terminal no puede recuperar la información que haya sido borrada intencionadamente por el usuario" (Betrán Pardo, art. cit.).

[29] La casación federal anuló una absolución en un caso de secuestro extorsivo, valorando como indicios de cargo, entre otros, que el acusado había eliminado casi todos los mensajes de WhatsApp de su celular, que del informe de extracción de datos del teléfono móvil se desprendían algunas conversaciones cortadas, lo que "daría cuenta que, tal como le solicitó su mujer, el nombrado eliminó casi todos los mensajes de WhatsApp de su dispositivo" (CFCP., Sala III, Reg. 759, 2/6/2021, "Sahonero Zapata").

tos informáticos o electrónicos con el objeto de secuestrar los componentes del sistema, obtener una copia o preservar datos o elementos de interés para la investigación, sin exigir notificación previa a la defensa ni encuadrarlo dentro del trámite de las pericias[30].

[30] CNacApelCrimyCorrec., Sala IV, 20/9/2019, "A., J. A. y otros s/nulidad".