elDial.com
Contenidos Jurídicos

Incautación y extracción de datos electrónicos almacenados en dispositivos móviles (evidencia digital) y su proyección en la defensa en juicio

Por Gustavo Eduardo Aboso[(*)]

Introducción

En el ámbito de la evidencia digital existen al menos dos técnicas de investigación orientadas hacia la extracción de datos electrónicos almacenados en dispositivos electrónicos (celulares, ordenadores) que obedecen a la misma finalidad de obtener prueba sobre el objeto del proceso penal, pero que representan una injerencia diferenciada en el ámbito de la privacidad personal. Nos referimos a la distinción existente entre la extracción de datos electrónicos de fuentes aportadas por la víctima, de la incautación compulsiva de datos de fuentes en poder del acusado.

El avance vertiginoso de la tecnología de la comunicación en la sociedad de la información incentivó la necesidad de adoptar regulaciones jurídicas más específicas en torno de la colección de prueba en el entorno digital en razón de la propagación de los sistemas de almacenamiento de datos electrónicos personales que erosionan de manera peligrosa los derechos humanos con especial atención de la zona de privacidad al quedar expuesta a la

(*) Doctor en Derecho (UNED- Madrid). Defensor de Cámara de Casación y Apelaciones en lo Penal, Penal Juvenil, Contravencional y de Faltas del Poder Judicial de la Ciudad Autónoma de Buenos Aires. Profesor de posgrado de Derecho Penal (UBA, Austral, Belgrano, Nacional de Nordeste, Nacional de Mar del Plata, Mendoza y del Salvador). Profesor invitado de la Universidad de Azuay (Ecuador) y la Universidad Mayor San Andrés (Bolivia). Autor del "Código Penal de la República Argentina comentado y concordado", 7.ª ed., 2025; "Derecho penal cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación ", Bdef, Montevideo-Buenos Aires, 2017; "Ciberdelitos. Análisis doctrinario y jurisprudencial", Vols. 1° (2023); 2° (2024) y 3° (2025), Ciudad Autónoma de Buenos Aires, elDial, Albremática, entre otras obras. Director del Suplemento de Derecho Penal y Procesal Penal de ElDial. Miembro Fundador de la Academia Argentina de Ciencias Penales.
Abreviaturas utilizadas: BGH = *Bundesgerichtshof* (Tribunal Superior de Justicia alemán). BVerfGE = *Bundesverfassungsgericht* (Tribunal constitucional alemán). CCAPPJCyF = Cámara de Casación y Apelaciones en lo Penal, Penal Juvenil, Contravencional y de Faltas. CFCCC = Cámara Federal de Casación en lo Criminal y Correccional. CJ = Corte de Justicia. CPP CABA = Código Procesal Penal de la Ciudad Autónoma de Buenos Aires. CNACC = Cámara Nacional de Apelaciones en lo Criminal y Correccional. ECHR = *European Court of Human Rights* (Tribunal Europeo de Derechos Humanos). LL = La Ley. STC = Sentencia del Tribunal Constitucional español. STS = Sentencia del Tribunal Supremo de Justicia español. STJ CABA = Superior Tribunal de Justicia de la Ciudad Autónoma de Buenos Aires. SWGDE = *Scientific Working Group on Digital Evidence*. TSJ = Tribunal Superior de Justicia.

cibervigilancia como lo recuerda la Asamblea General de Naciones Unidas sobre el derecho a la privacidad en la era digital al exhortar a los estados a que, entre otras cosas:

c) Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos electrónicos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos (...).[1]

Al mismo tiempo, el artículo 19 del Convenio sobre Cibercriminalidad (Budapest, 2001) regula el registro y la confiscación de datos informáticos almacenados y establece la necesidad de adoptar reformas legislativas adecuadas para facultar a las autoridades competentes a registrar o a tener acceso de un modo similar "a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos."

La legislación procesal penal regula en general la técnica de incautación de datos almacenados en dispositivos electrónicos como medio de investigación en el marco de la prueba digital. Algunos ejemplos de normas procesales que regulan esta actividad de investigación en entornos digitales son los artículos 151 del Código Procesal Penal Federal; 181 del Código Procesal Penal de la provincia de Corrientes; 199 del Código Procesal Penal de la provincia de Tucumán; 309 quater del Código Procesal Penal de la provincia de Salta (ley 8386); 183 del Código Procesal Penal de la provincia de Chubut; entre otros.

En los ordenamientos procesales que carecen de una norma específica que habilite la extracción de datos electrónicos se recurre a la norma genérica del registro de los objetos para salvar esta anomia.[2] Suele discutirse en la praxis forense cuál es la naturaleza de la acción de extraer datos del dispositivo electrónico de la víctima de amenazas, extorsión o cualquier otro comportamiento y su relación con el ejercicio de la defensa en juicio. Mientras que la legislación punitiva avanzó a pasos agigantados en la regulación especial de las conductas disvaliosas que tienen lugar en las redes o que atentan contra la integridad y el funcionamiento de los sistemas computacionales, la regulación procesal de la prueba digital no alcanzó el mismo vértigo normativo, siendo llamativo su retraso en vista de armonizar de manera integral el sistema penal.[3]

En una primera aproximación resulta conveniente hacer una matización que tiene por objeto en igual medida los datos electrónicos almacenados en un

[1] Resolución 68/167, de 18 de diciembre de 2013, aprobada en su sexagésimo octavo período de sesiones.

[2] Kerr, Orin S., Digital Evidence and the New Criminal Procedure, *Columbia Law Review*, Vol. 105, N° 1 (Jan., 2005), pp. 279 y ss. Como lo sostiene este autor es necesario la armonización de la legislación procesal para regular los medios de prueba en materia digital, ya que su naturaleza y forma de extracción difiere de la prevista para la evidencia material.

[3] Hilgendorf, Eric; Frank, Thomas y Valerius, Brian, *Computer-und Internetstrafrecht*, Ein Grundriss, Springer, Berlín, Heidelberg, 2005.

dispositivo electrónico, pero su titularidad habrá de determinar requisitos distintos. Nos referimos, en primer término, a los datos almacenados en un dispositivo del imputado, en cuyo caso resulta más adecuado hablar de "incautación de datos", ya que se parte de la base de la falta de colaboración o consentimiento de su titular, por lo tanto, la exigencia de la orden judicial deviene en una condición insoslayable por estar comprometido el ámbito de privacidad del afectado.[4]

Existen en las leyes procesales dispositivos que regulan esta contingencia y que parten de la misma base de asegurar el debido control judicial mediante la respectiva orden de incautación teniendo en cuenta que el afectado por la medida judicial se trata de una persona imputada de delito. En este caso las exigencias técnicas son mayores, ya que el objeto del proceso habrá de determinar la necesidad, la pertinencia y la razonabilidad de la injerencia en el ámbito de la privacidad del acusado. En consecuencia, el pedido fiscal de incautación de datos electrónicos debe estar respaldado por la comprobación indiciaria de los extremos del hecho investigado, la justificación del registro solicitado y el debido fundamento de su procedencia.[5] Un aspecto formal que debe tenerse en cuenta es que el acusador público debe precisar cuál será la técnica utilizada por perito informático para extraer los datos almacenados en el dispositivo, sentido y alcance de la búsqueda mediante programas debidamente individualizados para evitar exceder el objeto del proceso en su implementación.

Vale recordar que los datos electrónicos almacenados en el dispositivo del imputado y que son de interés para la investigación están alcanzados por la inviolabilidad de la privacidad, siendo indispensable el control judicial en la expedición de la orden de incautación del material sensible. Al respecto, la *Supreme Court of United States* sostuvo en los precedentes "Riley" y "Wurie", la importancia de resguardar la intimidad individual de las personas afectadas por las búsquedas realizadas por la autoridad policial sin la respectiva orden judicial, siendo un atentado contra la privacidad individual y, por ende, desencadenando la nulidad de lo actuado en consecuencia.

Idéntica tesitura adoptó el Tribunal Europeo de Derechos Humanos en el caso "Trabajo Rueda vs. España" al concluir que la búsqueda de la autoridad en el ordenador del imputado sin orden judicial representó un ataque a su intimidad personal derivada de la revisión compulsiva de archivos de imágenes almacenadas en su portátil.

A esto se le agrega el precedente "Bărbulescu v. Romania"[6] del mismo tribunal en el que se confirmó el área de protección de la intimidad en el uso de

[4] La supervisión judicial de la incautación de datos electrónicos está prevista en el artículo 15 del Convenio sobre la Ciberdelincuencia, suscrito en Budapest el 23 de noviembre de 2001 (Serie de Tratados Europeos n° 185), al decir: "2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardas incluirán una supervisión judicial u de otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento."

[5] SWGDE 16-F-002-2.1, Considerations for Required Minimization of Digital Evidence Seizure.

[6] ECHR, (GC), n° 61496/08), de 5/9/2017.

dispositivos electrónicos frente a la injerencia de particulares, en este caso, el empleador, que accedió al historial de búsquedas y correos electrónicos de su empleado para justificar el despido laboral.

Previo a continuar con el desarrollo de la temática abordada en este trabajo resulta necesario citar las disposiciones legislativas propuestas en torno de la incautación de datos electrónicos formulada recientemente por la Asamblea General de las Naciones Unidas en la resolución de 24 de diciembre de 2024 en el marco de la Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos[7]:

Artículo 28

Búsqueda e incautación de datos electrónicos almacenados
1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes a efectuar búsquedas:
a) En un sistema de tecnología de la información y las comunicaciones, en parte de él y en datos electrónicos almacenados en él; y
b) En un medio de almacenamiento de datos electrónicos en el que puedan estar almacenados los datos electrónicos que se busquen, o acceder a ellos de manera similar en el territorio de ese Estado parte.
2. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean
necesarias para garantizar que, cuando sus autoridades efectúen una búsqueda en un sistema de tecnología de la información y las comunicaciones específico o parte de él o accedan de manera similar a él, de conformidad con el párrafo 1 a) del presente artículo, y tengan motivos para creer que los datos electrónicos buscados están almacenados en otro sistema de tecnología de la información y las comunicaciones o parte de él en su territorio, y pueda accederse legalmente a esos datos a través del sistema inicial o esos datos estén disponibles para el sistema inicial, dichas autoridades puedan efectuar de manera rápida la búsqueda para obtener acceso a ese otro sistema de tecnología de la información y las comunicaciones.
3. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean
necesarias para facultar a sus autoridades competentes a incautarse de los datos electrónicos presentes en su territorio a que se haya tenido acceso de conformidad con los párrafos 1 o 2 del presente artículo u obtenerlos de manera similar. Estas medidas incluirán la facultad de:
a) Incautarse de un sistema de tecnología de la información y las comunicaciones o parte de él, o un medio de almacenamiento de datos electrónicos, u obtenerlo de manera similar;
b) Hacer y conservar copias de esos datos electrónicos en forma electrónica;
c) Mantener la integridad de los datos electrónicos almacenados pertinentes;

[7] Resolución 79/243. Convención de las Naciones Unidas contra la Ciberdelincuencia; Fortalecimiento de la Cooperación Internacional para la Lucha contra Determinados Delitos Cometidos mediante Sistemas de Tecnología de la Información y las Comunicaciones y para la Transmisión de Pruebas en Forma Electrónica de Delitos Graves.

d) Imposibilitar el acceso a esos datos electrónicos en el sistema de tecnología de la información y las comunicaciones al que se ha obtenido acceso o suprimirlos.
4. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean
necesarias para facultar a sus autoridades competentes a ordenar a toda persona provista de conocimientos sobre el funcionamiento del sistema de tecnología de la información y las comunicaciones en cuestión, la red de información y telecomunicaciones o sus componentes o las medidas aplicadas para proteger los datos electrónicos que figuran en ellos que proporcione, según resulte razonable, la información necesaria para que puedan aplicarse las medidas mencionadas en los párrafos 1 a 3 del presente artículo.

La extracción de datos electrónicos de fuentes de la víctima

Por lo común la víctima de delitos cometidos mediante el uso de medios telemáticos suele poner a disposición de la autoridad judicial el dispositivo de su propiedad para proceder a la extracción de los datos incriminadores. Por ejemplo, cuando se trata de una víctima de amenazas, *in fortiori*, en el contexto de la violencia de género, el contenido enviado mediante la mensajería de correo sirve para acreditar los extremos de la denuncia. De esta manera, la extracción de los hilos de conversación de la aplicación WhatsApp en la que el imputado amenaza de manera reiterada a la víctima constituye una forma de prueba aceptada en la praxis forense.

La distinción obligada en esta situación es que la víctima entrega de manera voluntaria el dispositivo en el que se encuentra almacenada la prueba digital con el objeto de comprobar la identidad del remitente y el contenido amenazante necesarios para la formalización de la denuncia. Acá no se requiere orden judicial, porque el propio ofendido es el que pone de manera voluntaria a disposición de la autoridad el contenido de los datos y tampoco se lesiona la intimidad del remitente, es decir, del acusado, porque no rige acá el secreto de las comunicaciones y menos aún la afectación de su intimidad cuando utiliza el medio electrónico para amenazar a otro.[8]

Como primera conclusión podemos aseverar que la entrega voluntaria de la prueba del delito denunciado por parte de la víctima o un tercero, v. gr., los representantes parentales cuando se tratare de un menor de edad, ni lesiona ni menoscaba el derecho a la intimidad ni el secreto de las comunicaciones cuando son utilizadas como medio idóneo para cometer la conducta disvaliosa.[9]

Es lícita la entrega del dispositivo efectuada por la madre de la víctima menor de edad con el objeto de acreditar las comunicaciones recibidas por el acusado

[8] CCAPPJCyF, Sala 2, causa nº 1707-00-CC/2017, “B, A. E y otros”, de 6/10/2017.
[9] CNACC, Sala 4, causa Nº 33.396/2019, “P., R. E.”, de 27/9/2021; CCAPPJyF, Sala 3, por mayoría, causa n° 27.690-02-00/12, “D., C. M.”, de 15/12/2014.

de abuso sexual y la experticia efectuada sobre su contenido vinculado con los mensajes enviados mediante el sistema de mensajería instantánea.[10]

Hemos señalado anteriormente que una simple operación de copiado, transmisión o transcripción de datos electrónicos almacenados en un dispositivo electrónico proporcionado con el consentimiento de su titular, es decir, nos referimos a la víctima o testigo, haría innecesaria la intervención de la contraparte.[11]

En el contexto de violencia de género, la entrega voluntaria del dispositivo en el que la víctima recibió los mensajes fraudulentos con el objeto de perfeccionar la estafa mediante el sistema de mensajería WhatsApp no le irroga a los intereses de la defensa ningún perjuicio el hecho de que la evidencia haya sido obtenida sin mediar pericia informática. En este sentido, la defensa no pudo demostrar que la prueba haya sido alterada en algún modo para perjudicar al acusado.[12] Por consiguiente, la notificación cursada a través del medio electrónico se consideró válida en relación con la comisión del delito de desobediencia de una medida cautelar de prohibición de contacto con la víctima en el marco de un proceso, en cuyo caso debe acreditarse que el imputado estaba en pleno conocimiento de la prohibición de contacto.[13]

Precisamente el sistema de mensajería instantánea ha sido incluido entre los medios de notificación válidos cuando se trata de efectuar las diligencias judiciales necesarias vinculadas con la notificación de medidas preventivas o asegurativas en favor de la víctima de violencia de género.[14]

Un aspecto controvertido de esta forma de obtención probatoria se vincula con la necesidad de notificar a la defensa del acusado sobre su ejecución, ya que se discute sobre su naturaleza técnica, es decir, si se trata de un mero informe o una pericia en sentido estricto, siendo necesario en este último caso la debida notificación de la defensa, bajo pena de nulidad.

Un sector mayoritario de la doctrina judicial nacional sostiene que su naturaleza se corresponde con el informe o examen técnico, siendo innecesario la previa notificación a la defensa.[15] En especial, cuando el medio técnico está orientado hacia la comprobación de la autenticidad de la comunicación entablada entre el autor y su víctima, se afirmó que la participación del cuerpo de especialistas en el área se limitó a la extracción y conservación de los datos almacenados en el dispositivo entregado voluntariamente por la víctima destinataria de las amenazas, por lo tanto, no tuvo el sentido ni el alcance de una pericia

[10] STS, Sala de lo Penal, 3341/2025, de 3/7/2025.
[11] Aboso, Gustavo E., *Código Procesal Penal de la Ciudad Autónoma de Buenos Aires comentado y concordado con jurisprudencia y doctrina nacional y extranjera*, 1.ª ed., Albremática, Ciudad Autónoma de Buenos Aires, 2024, p. 303, con cita del precedente de la CNACC, Sala IV, causa n° 33.396/19. “Pagnotta, R. E.”, de 27/9/2021.
[12] CNACC, Sala 4, causa n° 6.894/24, “Casco, J. I.”, de 2/6/2025.
[13] CAPPJCYF, Sala 1, causa n° 17164-2020-2, “I.J.E.”, de 23/11/2021.
[14] CNACC, Sala 5, causa n° 111/23, “Monzón, F. M.”, de 24/5/2024.
[15] CNACC, Sala 4, CCC 81978/2018/11/CA9, “A., J. A.”, de 20/9/2019, con nota de Carla Paola Delle Donne, *LL*, 2020-A, pp. 232 y ss.; causa Nº 33.396/2019 , “P., R. E.”, de 27/9/2021.

informática en un sentido estricto, en atención a lo previsto en el artículo 253 del Código Procesal Penal de la Nación.[16]

Recordemos que el citado artículo establece que:

Facultad de ordenar las pericias

Art. 253. - El juez podrá ordenar pericias siempre que para conocer o apreciar algún hecho o circunstancia pertinente a la causa, sean necesarios o convenientes conocimientos especiales en alguna ciencia, arte o técnica.

A su vez, el artículo 258 de la misma ley adjetiva dispone:

Nombramiento y notificación

Art. 258. - El juez designará de oficio a un perito, salvo que considere indispensable que sean más. Lo hará entre los que tengan el carácter de peritos oficiales; si no los hubiere, entre los funcionarios públicos que, en razón de su título profesional o de su competencia, se encuentren habilitados para emitir dictamen acerca del hecho o circunstancia que se quiere establecer.
Notificará esta resolución al ministerio fiscal, a la parte querellante y a los defensores antes que se inicien las operaciones periciales, bajo pena de nulidad, a menos que haya suma urgencia o que la indagación sea extremadamente simple.
En estos casos, bajo la misma sanción, se les notificará que se realizó la pericia, que puedan hacer examinar sus resultados por medio de otro perito y pedir, si fuere posible, su reproducción.

Si se tratare de una pericia informática, el juez está obligado a notificar a las partes interesadas a los fines de que puedan proponer perito de parte, bajo apercibimiento de nulidad.

En cambio, cuando se sostiene que la extracción y la conservación de datos almacenados en el dispositivo de la víctima carece de tal naturaleza, aplicándose en consecuencia el contenido del artículo 233 de ese mismo texto legal que dispone:

Custodia del objeto secuestrado

Art. 233. - Los efectos secuestrados serán inventariados y puestos, bajo segura custodia, a disposición del tribunal. En caso necesario podrá disponerse su depósito.
El juez podrá ordenar la obtención de copias o reproducciones de las cosas secuestradas cuando éstas puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la instrucción.

---

[16] CNACC, Sala 1, causa n° 1132462/2025, “Casinelli, E.”, de 25/6/2025; Sala 4, CCC81978/2018/11/CA9, “Amarilla, J.A.”, de 20/9/2019; Sala 5, CCC 35.856/2023/CA3, “Teper, C. G.”, de 21/8/2025, con nota de Bura Peralta, Javier E., “”Nulidad por falta de notificación a la defensa en extracciones forenses”, elDial.Express, de 18/9/2025.

Las cosas secuestradas serán aseguradas con el sello del tribunal y con la firma del juez y secretario, debiéndose firmar los documentos en cada una de sus hojas.
Si fuere necesario remover los sellos, se verificará previamente su identidad e integridad. Concluido el acto, aquéllos serán repuestos y de todo se dejará constancia.

Por el contrario, a partir de que en la jurisdicción local rige el sistema acusatorio desde que la Constitución de la Ciudad Autónoma de Buenos Aires estableció que ese sistema procesal es el único admisible constitucionalmente (artículo 13.3), los informes y las pericias forenses integran el arco probatorio a disposición del agente fiscal en el marco del ejercicio de sus atribuciones propias de investigación (artículo 113 del CPP CABA), comúnmente acuñado bajo el término de "amplitud probatoria". La ley procesal penal local le reconoce al fiscal la facultad de requerir informes y peritajes (artículo 100 del texto citado) u ordenar pericias forenses (artículo 136 del texto citado), debiéndose asegurar la debida participación del acusado, su defensa y la querella cuando así se disponga (artículo 103 ob. cit.).

Ya hemos señalado que las facultades de investigación en cabeza de los representantes del Ministerio Público Fiscal reconocen de modo necesario en el marco de un proceso con todas las garantías de ciertas limitaciones que le impiden ejercer la titularidad de la acción penal de manera arbitraria, ya que la mencionada amplitud probatoria debe satisfacer el test de legalidad en la regulación de los medios probatorios lícitos, amén de que son la reglamentación de las garantías y los derechos judiciales asegurados en nuestra constitución y el bloque de convencionalidad.[17]

Una situación distinta se presenta cuando se omitió de manera deliberada la notificación de las partes para participar en la pericia bajo el sutil argumento de que se trataba de un mero informe cuando en realidad la técnica aplicada denotó la ejecución de una pericia forense.[18]

En el ámbito local, a partir de la Resolución n° 238/2020 del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, de 11/11/2020, se puso en funcionamiento el Protocolo de Digitalización de Expedientes Judiciales y en su Anexo se establece el trámite a seguir para asegurar su correcta implementación. Si se notificó en tiempo y forma sobre la fecha y hora de la realización de la pericia informática, los puntos de análisis y se le facilitó el acceso al expediente digital con la prueba de respaldo, no cabe acoger el pedido nulificante de la pericia practicada por parte de la defensa si su falta de supervisión obedeció a su propia culpa profesional.[19]

La conservación de objetos para evitar su alteración resulta adecuada para asegurar la intangibilidad de los datos digitales, pero a diferencia de los objetos materiales, en el caso de los contenidos sintéticos la cuestión debe ser

[17] Aboso, *Código Procesal Penal de la Ciudad Autónoma de Buenos Aires*, pp. 236 y ss.
[18] CNACC, Sala VII, causa n° 42.058/2021, "Parga, C. D. s/nulidad", de 4/10/2023.
[19] CCAPPJCyF, Sala I, causa n° INC 47207/2019-1, "NN", de 24/11/2020; CNCC, Sala VI, causa n° 48.669/18, "Carhuanca Vilchez", de 27/5/2020.

analizada desde una perspectiva distinta porque acá se debe utilizar de manera indefectible un programa informático para la extracción y la conservación de la prueba digital. Por lo tanto, la operación resulta ser más compleja y el uso de programas especialmente diseñados para tal fin puede incidir en la misma intangibilidad probatoria que se quiere resguardar.

Esta situación está expresamente regulada en las leyes procesales a los efectos de posibilitar una contraprueba del material peritado (v. gr., artículo 140 CPP CABA).

Una situación particular se presenta cuando la propia víctima es la que aporta la evidencia digital al proceso, por ejemplo, mediante la reproducción de las imágenes de pantalla de las comunicaciones mantenidas con el denunciado con el objeto de acreditar las amenazas. Al no mediar la convocatoria de un perito, se ha relativizado su valor probatorio[20], salvo que el imputado haya reconocido su autoría.[21]

Cuando se trata de evidencia digital la defensa del acusado suele encarrilar su queja sobre la autenticidad del contenido de la comunicación bidireccional, su autoría o directamente apelar a la inobservancia de la cadena de custodia. En cualquier caso corresponde que la defensa haya accionado los medios probatorios adecuados para comprobar los extremos denunciados y no caer en la mera retórica, por lo tanto, habrá de proponer las pruebas necesarias para comprobar los extremos denunciados.[22]

La naturaleza de la evidencia digital requiere la actuación de peritos o especialistas en el área informática mediante el uso de herramientas informáticas más o menos complejas con el objeto de asegurar y conservar la prueba, pero la técnica aplicada sin duda que demanda un conocimiento específico que dista de ser uno común, *in fortiori*, cuando las leyes procesales sostienen la necesidad de establecer una cadena de custodia en función de la intangibilidad de la prueba, su ductilidad y alterabilidad.[23]

Como se expuso al principio de este trabajo, la Resolución 79/243 aprobada por la Asamblea General de las Naciones Unidas, en su artículo 28, *in fine*, subraya la necesidad de la intervención de personal con “conocimientos sobre el funcionamiento del sistema de tecnología de la información y las comunicaciones en cuestión, la red de información y telecomunicaciones o sus componentes o las medidas aplicadas para proteger los datos electrónicos que figuran en ellos que proporcione, según resulte razonable, la información necesaria para que puedan aplicarse las medidas mencionadas en los párrafos 1 a 3 del presente artículo.”

Como lo expone la doctrina especializada el avance de las nuevas tecnologías impuso al mismo tiempo el surgimiento de una nueva forma de investigación

[20] CCAPPJCyF, Sala III, causa n° 10114/2020-3, “Lorenzi, L. M.”, de 15/2/2023.
[21] CCAPPJCyF, Sala II, causa n° 2242786/2023, “Durante, M.”, de 22/9/2023.
[22] STS, Sala de lo Penal, 2949/2018, de 19/7/2018.
[23] CFCCC, Sala IV, causa n° 16.339, “Gil, J. s/ recurso de casación”, Reg. n° 337/13, de 22/4/2013.

basada en el tratamiento de los datos electrónicos almacenados en los dispositivos electrónicos de los acusados que suelen abarcar miles de gigabytes o terabytes que requieren a su vez de la participación de especialistas y recursos dinerarios para poder solventar una estructura cada vez más extensa de departamentos dedicados al estudio de la evidencia digital.[24]

Esta inversión en recursos técnicos y humanos acrecienta al mismo tiempo la relación asimétrica que existen entre el Ministerio Público Fiscal y la Defensoría Pública en la elaboración de los presupuestos anuales para el equipamiento y la contratación de expertos, lo que culmina con la necesidad de contratar de manera individual peritos de parte para algún grupo de procesos penales, que en el caso de los letrados particulares se transforma directamente en una posibilidad lejana dependiendo de la capacidad económica del cliente.[25]

Del mismo contenido del Protocolo para la identificación, recolección, preservación, procesamiento y presentación de la evidencia digital elaborado por el Ministerio Público Fiscal de la Nación surge los pasos que deben seguirse en el tratamiento de los datos almacenados en dispositivos electrónicos.[26] La intervención de personal especializado es la regla, en especial, en los albores de la investigación cuando se secuestran mediando orden judicial los elementos que pueden ser de interés para el objeto del proceso y guardan relación de afinidad con su naturaleza. En el caso del triaje para la identificación de los elementos digitales de interés para la instrucción, la mediación de técnicos especializados es indispensable.[27]

En general, la convocatoria de personal técnico especializado es la regla, no la excepción, en razón de la naturaleza del potencial elemento de prueba digital (PEP digital).[28]

A modo de graficar aún más la situación analizada nos permitimos extractar la sección del citado protocolo que establece los pasos a seguir en el secuestro del dispositivo y el aseguramiento de la prueba digital, por ejemplo, cuando el aparato se encuentra encendido (CALIENTE-AFU):

“a. Realizar la extracción de la tarjeta SIM para prevenir el acceso o modificación remota a través de la red de telefonía celular (3G, 4G, 5G, etc.).
b. Registrar la numeración y logo visibles en el exterior de la tarjeta SIM (ICCID).
c. En caso de observarse más de un slot de SIM en el dispositivo, identificar y registrar el slot en el que se encontraban colocadas cada una de las tarjetas SIM.
d. Adherir la o las tarjetas SIM con cinta transparente a la carcasa del equipo.

[24] Turner, Jenia I, “Managing Digital Discovery in Criminal Cases”, *The Journal of Criminal Law and Criminology* (1973-), Vol. 109, N° 2 (2019), pp. 237 y ss., pp. 249 y ss.
[25] Turner, “Managing Digital Discovery in Criminal Cases”, pp. 251 y ss.
[26] Ministerio Público Fiscal y Ministerio de Seguridad (2023).
[27] Ib., 4.1. y siguientes.
[28] Ob. cit., 3.1.

e. De ser posible, identificar el IMEI del dispositivo telefónico. En el caso de que no se visualice, registrar “IMEI no visible / ilegible”. Por ningún motivo se deberá manipular el equipo con la intención de obtener número de serie/IMEI con métodos tales como ingresando el código “*#06#” en el teclado o ingresando a su menú de configuración
f. De ser posible, activar el modo avión del dispositivo.
g. De ser posible, desactivar la opción de WIFI.
h. De ser posible, identificar y registrar marca o inscripción visible (se puede observar en la carcasa del dispositivo o impreso en la etiqueta de datos). En el caso que no se visualice, registrar “Marca o Inscripción No visible”.
i. De ser posible, identificar y registrar modelo técnico (se puede observar en la carcasa del dispositivo o impreso en la etiqueta de datos). En el caso que no se visualice, registrar “Modelo Técnico No visible”.
j. De ser posible, identificar Número de Serie (se puede observar en la carcasa del dispositivo, impreso en la etiqueta de datos ubicada generalmente bajo la batería cuando la misma sea accesible). En caso de no observarse, por ningún motivo se deberá manipular el equipo con la intención de obtener el número de serie con métodos tales como ingresando el código “*#06#” en el teclado o ingresando a su menú de configuración.
k. De existir Tarjeta de Memoria consignar el tipo, capacidad e inscripción observada. En caso de no existir, registrar “No Posee Tarjeta de Memoria”.
l. Registrar el estado de conservación a simple vista del dispositivo (Bueno, Regular, Malo) incluyendo descripción de detalles. Por ejemplo, cuando posea un faltante de partes o pantalla fracturada se considerará un estado de conservación malo.
m. Finalizados los pasos anteriores, colocar el dispositivo en una bolsa Faraday o desplegar otro método no invasivo que se valga del mismo principio para lograr un aislamiento electromagnético de toda señal (Ej. papel aluminio. Utilizar como mínimo 5 vueltas sobre el dispositivo).”

Este procedimiento de manejo, extracción y preservación de datos almacenados en dispositivos móviles sigue las recomendaciones elaboradas por asociaciones de profesionales en evidencia forense digital que establecen los pasos que deben seguirse para asegurar la intangibilidad del material informático objeto de la pericia. Las pautas incluyen desde la identificación primaria del dispositivo electrónico mediante fotografía, estado de conservación, número de serie de fabricación, entre otras, hasta el aislamiento del aparato para evitar cualquier forma de intromisión remota.[29]

Recuérdese que cuando se habla de autenticidad de la evidencia digital se pone el foco en tres aspectos esenciales, a saber: a) autenticación (*Authentication*), esta es la capacidad de demostrar que el objeto digital es lo que pretende serlo. La autenticidad de un objeto digital se preserva mediante el uso de técnicas para evitar que los datos sean manipulados, alterados o falsificados deliberada o inadvertidamente; b) integridad (*Integrity*), que se vincula con qué tan sólidos son los datos, como si los datos están dañados de alguna manera y si están completos, ya que poseen todas las partes y enlaces necesarios. La integridad no es una condición absoluta, sino un estado de

[29] SWGDE 18-F-003-2.0, Best Practices for Mobile Device Evidence Collection & Preservation Handling and Acquisition.

relaciones, y si se logrará la carga de la prueba en un caso individual dependerá de la solidez de las relaciones con los datos; y, por último, c) fiabilidad (*Reliability*) es la capacidad de un objeto digital para representar los hechos a los que se refiere pretende atestiguar, lo que a su vez está vinculado a garantizar una atributos técnicos (incluida una combinación de pautas preventivas, como para evitar modificaciones y cambios no autorizados, y de verificación proporcionar un grado de garantía en cuanto a la identidad de los usuarios y la provisión de las pistas de auditoría del documento cuando se visualizan y manipulan los datos) y trabajando para proporcionar un grado de garantía de que el objeto digital pueden considerarse confiables. En esencia, la confiabilidad está asociada con el grado.[30]

Un argumento poco convincente que suele emplearse para consustanciar la idea de que el informe no exige la participación de la defensa es que su sencillez no demanda especialidad alguna, es decir, se trata de un simple comprobación del estado de las cosas.[31] Disentimos con esta apreciación, en especial, porque toda extracción de datos de imágenes, vídeos, textos o audiovisuales conlleva de manera necesaria el uso de programas especialmente diseñados a tal efecto, sumado a que la naturaleza inmaterial de los datos digitales puede acarrear la alteración o directamente la pérdida total o parcial de la información. La propia selección de los audios o textos enviados mediante mensajería puede desembocar en una selección arbitraria que tuerza su interpretación y el contexto ambiental en la que se materializaron.

Apoya nuestro punto de vista la bibliografía en materia de evidencia forense en materia digital (*Digital Forensics*) que subraya la orientación seguida en el marco de las investigaciones judiciales que requieren de manera progresiva un conocimiento y técnica especializada en el tratamiento y almacenamiento de datos con el objeto de ser empleados como medios de prueba en un proceso penal al decir:

“Los rápidos desarrollos en tecnología y delitos relacionados con la informática han creado una demanda significativa de personas que puedan recopilar, analizar e interpretar evidencia digital. Específicamente, existe una creciente necesidad de profesionales calificados en las siguientes tres áreas generales de especialización: preservación de evidencia digital, extracción de información utilizable de evidencia digital e interpretación de evidencia digital para obtener información sobre aspectos clave de un delito. Estas especializaciones no se limitan a la aplicación de la ley y también se han desarrollado en el mundo corporativo. Incluso cuando una sola persona es responsable de recopilar, analizar e interpretar evidencia digital, es útil considerar estas tareas por separado. Cada área de especialización requiere diferentes habilidades y procedimientos, y tratarlos por separado facilita la definición de la formación y los estándares en cada área.”[32]

---

[30] Mason, Stephen; Stanfield, Allison, 7 Authenticating electronic evidence, *Electronic Evidence*, University of London Press, 2017, pp. 193 y ss.

[31] CCAPPJCyF, Sala 1, causa n° 1461166/2025, “Colucci González, G. L.”, de 14/8/2025.

[32] Casey, Eoghan, *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, Third Edition, Academic Press, 2011, p. 11. En el derecho penal chileno se expone con solvencia la actual situación jurídica mediante la sanción de la ley 21.459 en la obra *Delitos*

Lo dicho viene reforzado por el uso de instrumentos digitales como el sistema *Universal Forensic Extraction Device* (UFED) que sirve para la extracción de los datos de interés almacenados en la memoria del dispositivo de la víctima. El uso de esta clase de sistemas informáticos demanda la concurrencia de expertos que permitan asegurar la intangibilidad y la conservación de la prueba obtenida. También debe recordarse que uno de los usos más aplicados de este sistema consiste en el desbloqueo de dispositivos electrónicos, cuyas capas de seguridad pueden derivar en la pérdida de la información requerida.

Tomando como ejemplo el informe sobre el estado de conservación de un objeto material, por ejemplo, un arma de fuego[33], un cuchillo[34], un animal[35] o la rotura de un objeto[36], en el que no existe duda sobre la falta de necesidad de efectuar un examen más exhaustivo sobre ese elemento, ya que la constatación de su estado se revela como una simple actividad en la que el observador se limita a describir la forma, su estado y si presenta alguna alteración significativa en relación con la naturaleza del objeto en el proceso.

Por el contrario, la lectura del contenido de los protocolos aplicables a la extracción de datos de un dispositivo electrónico requiere, por un lado, la especialidad del operador, es decir, debe tratarse de un profesional con conocimiento especial sobre la materia; por el otro, no existe una mera descripción del objeto, en nuestro caso, inmaterial, como sucede cuando se trata de un elemento material, sino que es menester utilizar programas especialmente diseñados para el registro de los datos almacenados en el hardware que lejos está de ser una tarea sencilla. Ya el empleo de técnicas cada vez más sofisticadas de registros digitales evidencia que lejos de tratarse de un mero informe descriptivo obtenido mediante los sentidos.

Dista de la creencia común de que el uso de las herramientas forenses en materia digital aplicadas a la extracción de datos almacenados en un dispositivo electrónico se limita a la mera copia de datos y así la simplicidad de tal técnica la diferencia de la pericia propiamente dicha. Se ha dicho que “la extracción no es simplemente desplazarse por mensajes de texto o copiar archivos de un disco duro, aunque tales actividades a menudo representan la primera etapa del proceso de extracción. Las técnicas manuales implican el uso de entradas estándar incluidas o integradas en el dispositivo, como pantallas táctiles o teclados. Este es el nivel más básico de extracción, ya que no requiere herramientas especializadas, aunque el conocimiento de la estructura de archivos y los sistemas operativos ayudará considerablemente en el análisis. La extracción manual permite el acceso solo a la información disponible a través de la interfaz estándar. Por ejemplo, los elementos eliminados no se podrían obtener a través de este proceso, ya que los

---

informáticos y cibercriminalidad. Aspectos sustantivos y procesales, de Laura Mayer Lux y Jaime Vera Vega, Actualidad Criminológica y Penal, N° 15, Bdef, Montevideo-Buenos Aires, 2024, en especial, pp. 353 y ss. que versa sobre las reglas procesales contenidos en la citada ley.

[33] CCAPPJCyF, Sala 4, causa n° 1761191/2023, “R., L. I.”, de 26/7/2023.

[34] CCAPPJCyF, Sala 1, causa n° 23.645/2019-1, “O., O. Y.”, de 24/6/2019.

[35] CCAPPJCyF, Sala 2, por mayoría, causa n° 14212892/2020, “Galeano, J. E.”, de 5/2/2020.

[36] CCAPPJCyF, Sala 1, causa n° 2431/2018-1, “Robledo, R. P.”, de 12/12/2018.

clústeres de archivos eliminados no se pueden explorar a través de operaciones básicas de apuntar y hacer clic. Este nivel de procesamiento es comparable a sentarse frente a una computadora buscando un archivo en particular explorando carpetas de archivos con un mouse y un teclado."[37]

Resulta oportuno citar en este caso el propio protocolo implementado por el citado Ministerio Público Fiscal de la Nación y que fue elaborado en virtud de las indicaciones brindadas por los técnicos informáticos que permiten concluir de manera prístina que estamos lejos de un mero examen o constatación y más próximos a una auténtica pericia. La especialidad que debe tener el técnico sumado a las herramientas digitales de investigación aplicadas a los dispositivos con el objeto de extraer la información útil y necesaria para la investigación judicial no indican otra cosa de que se trata de una pericia, en los términos acuñados en la ley procesal.[38]

Por lo demás, algunos tribunales entienden que la delimitación del informe de la pericia resulta ser una controversia menor, ya que aun siguiendo este último criterio la cuestión habrá de resolverse al momento de la ponderación de la prueba en la sentencia. Será entonces el juez de juicio el que deberá asignar mayor o menor entidad a la evidencia digital cuya extracción y autenticidad se critica.[39] Esta postura no resulta convincente ya que opta por diferir la potencial violación de la defensa en juicio al momento del debate sin atender a los aspectos centrales como el de la posibilidad de reproducir la prueba, aunque también debe señalarse que la mera invocación de tal afectación resulta estéril si la defensa no solicitó la contraprueba o su agravio se sustancia en la mera disconformidad con lo resuelto.

Un matiz saliente de la incautación de datos de fuentes aportadas por la víctima está vinculado con la necesidad de establecer límites claros de registro para evitar lo que se conoce coloquialmente como "excursión de pesca". Al respecto, se declaró la nulidad parcial de la transcripción de los mensajes cursados entre el acusado y la víctima de amenazas obtenidos de su dispositivo electrónico que fuera entregado de manera voluntaria porque el personal técnico se excedió en la búsqueda y abarcó de manera arbitraria otros correos de mensajería con otros usuarios que no estaban sindicados en la orden primigenia.[40]

El registro de una comunicación en el marco del cumplimiento de medidas de precaución o reglas de conductas voluntariamente asumidas

[37] Goodison, Sean E., Davis, Robert C. and Jackson Brian A., Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, en *Digital Evidence and the U.S. Criminal Justice System*, Rand Corporation, 2015, pp. 5 y ss.

[38] *Código Procesal Penal de la Ciudad Autónoma de Buenos Aires. Análisis doctrinal y jurisprudencial*, (Marcela De Langhe dirección), 2.ª ed., t. 1 (arts. 1° - 207), Hammurabi, CABA, 2023, comentario del Capítulo V, del Libro II, pp. 473 y ss., con comentario de Miguel Kessler.

[39] CCAPPJCyF, Sala 2, causa n° 1707-00-CC/2017, "B., A. E.", de 6/10/2017; Sala 3, causa n° 16.990-00-00/13, "L., C. M.", de 31/3/2015.

[40] CCAPPJCyF, Sala 2, causa n° 19142-00-CC/2015, "A,. M .E.", de 5/10/2017.

Cuando el imputado aceptó someterse a la observancia de ciertas reglas de conducta que implican la de abstenerse de comunicarse con la denunciante en el marco del cumplimiento de una suspensión del proceso a prueba, o bien ella fue impuesta de manera compulsiva por el juez en el ámbito de un proceso civil o penal por violencia de género, la comprobación de su conducta autolimitante o coercitiva no afecta la intimidad ni el secreto de las comunicaciones.[41] En primer término, cuando la víctima aportó su dispositivo para la certificación de la inobservancia de la prohibición de contacto telemático, el probado o destinatario de la cautelar de protección no puede alegar la violación de su privacidad, en especial, porque el registro del número de abonado, la fecha y hora de la comunicación y su duración registradas en el sistema no acarrea perjuicio alguno.

El registro de llamadas salientes y entrantes de un abonado, la víctima, en el servicio de mensajería instalado en su dispositivo no se considera una comunicación en línea, sino tan solo un registro de esa comunicación pasada. Por lo demás, que sea la propia denunciante la que aportó como prueba dirimente en el incumplimiento de la orden judicial o la regla de conducta importa cuánto mucho una renuncia a su propia privacidad, en consecuencia, no existe una injerencia arbitraria por parte de la autoridad judicial.[42]

Una línea jurisprudencial entiende que el momento oportuno para debatir sobre la naturaleza y la validez del informe realizado por el perito informático debe ser durante el debate, ya que ahí recién la defensa tendrá la oportunidad para examinar al perito sobre la técnica utilizada, la selección de los datos pesquisados, su cantidad y las conclusiones pertinentes.[43]

Sólo por citar un ejemplo, en el precedente “Zerrizuela, J. R.” del Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires se rechazó el recurso de queja interpuesto por la defensa del acusado por lesiones dolosas en un contexto de violencia de género que se basó, entre otros aspectos, sobre el rechazo del pedido de peritación del dispositivo celular de la víctima que había aportado a la investigación imágenes de pantallas de los mensajes enviados por el sindicado que permitirían dar verosimilitud a su testimonio. La máxima instancia local rechazó el remedio procesal directo bajo el argumento de que se trataba de una cuestión de hecho y prueba ajena a la competencia del tribunal, sumado a que el recurrente no pudo demostrar el agravio concreto que el rechazo de la medida procesal le había ocasionado.[44]

Incautación de datos en dispositivo electrónico del imputado y la necesidad de la orden judicial

[41] CCAPPJCyF, Sala 1, causa n° 754791/2021, “P., K. G.”, de 5/5/2021.
[42] CCAPPJCyF, Sala 1, causa n° 28.760-00-CC/11, “P. R. I.”, de 5/8/2013.
[43] CCAPPJCyF, Sala 2, causa nº 1707-00-CC/2017, “B, A. E y otros”, de 6/10/2017.
[44] TSJ CABA, expte. n° QTS 11805/2020-5, “Zerrizuela, J. R. s/ Queja por recurso de inconstitucionalidad denegado en Zerrizuela, J. R. sobre 89 – Lesiones leves y otros”, de 12/10/2022.

A diferencia de la entrega voluntaria de evidencia digital por parte de la víctima del delito (*extracción de datos*), en el caso de la persona acusada de delito la situación jurídica es distinta ya que ella se encuentra amparada por las garantías judiciales que hacen necesario la autorización judicial para proceder a la incautación de datos electrónicos, salvo que el acusado haya entregado de manera voluntaria el registro de las conversaciones mantenidas con una tercera persona para demostrar su desconocimiento de la falsedad de la licencia de conducir que se le atribuyó.[45]

En el ambiental digital son numerosas las conductas disvaliosas que tienen lugar vinculadas con la transmisión de datos electrónicos que tienen relevancia típica, sin ánimo de pretender ser exhaustivos en el tema podemos citar que las amenazas proferidas a través del sistema de mensajería instantánea (v. gr., WhatsApp[46]), el uso de las redes telemáticas para la distribución de material de abuso sexual infantil[47] o el acoso sexual de menores de edad[48] representan sin duda los casos más conocidos en el universo delictivo del uso de las redes informáticas para la comisión de delitos. De ahí que la evidencia digital aparezca de manera preponderante y en función de la naturaleza técnica del delito cometido como el medio de prueba excluyente sobre el que se cierne cualquier investigación judicial.

Numerosos homicidios han sido aclarados a partir del uso de técnicas de investigación digitales que permitieron la colección de datos de historial de búsqueda en internet sobre métodos y sustancias para provocar la muerte sin sospecha o la geolocalización de los sospechosos el día del hecho.[49] La evidencia digital no se distingue en su concepto de otro tipo de evidencia física, pero a diferencia de esta última el registro y colección de datos resulta distinta al incorporar técnicas informáticas de investigación orientadas hacia el registro digital.[50]

---

[45] CNACC, Sala 5, CCC 27678/2022/CA1, “Ibarra, D. S.”, de 10/8/2022.

[46] Sobre la valoración de la prueba informática obtenida de la fuente de WhatsApp en el proceso civil, penal, comercial y laboral, cfr. *E book: E-Mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías*, Horacio R. Granero (dirección), María Rosa Steckbaner (coordinación), Derecho Procesal Informático, 1.ª ed., Albremática, Ciudad Autónoma de Buenos Aires, 2019, pp. 75 y ss., pp. 121 y ss., pp. 189 y ss., pp. 267 y ss., pp. 323 y ss., pp. 389 y ss., pp. 421 y ss.

[47] CCAPPJCyF, Sala 2, causa n° 689465/2023, “F., C.”, de 29/3/2023. Los delitos de tenencia, distribución y difusión de material de abuso sexual infantil (MASI) reflejan el impacto de la tecnología de las comunicaciones en el marco de la prueba en un proceso penal. El objeto de las acciones típicas de esta norma de conducta tienen como patrón la disponibilidad técnica de archivos de imágenes o vídeos de abuso y explotación sexual de menores de edad. Al respecto, Aboso, Gustavo E., “El uso de la Inteligencia Artificial (IA) para la generación de deep fakes en el tráfico de material de abuso sexual infantil y la anomia en el sistema penal argentino (artículo 128 del Código Penal Argentino). La necesidad de una urgente reforma”, publicado en el *Suplemento Penal y Procesal Penal de El Dial*, el 21/8/2025 [Cita online: DC3682].

[48] CJ Catamarca, expte. N° XXX/20, “S. P. J, P. – grooming s/ recurso de casación”, de 14/6/2021.

[49] CFCCC, Sala 1, causa n° CCC 45425/2007/TO1/CFC6, “Schlenker, A. y otros s/ recurso de casación”, Reg. n° 846/16.1, 17/5/2017.

[50] Goodison et al., Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, pp. 1 y ss.

En esta línea debemos citar los casos “Riley”[51] y “Wurie”[52] de la Corte Suprema de Justicia de los Estados Unidos que establecieron la necesidad de la orden judicial para practicar una búsqueda en el celular de los acusados. De acuerdo a los fundamentos del precedente citado, cualquier búsqueda de información o datos electrónicos asociados a la eventual comisión de delitos debe estar precedida por el pedido fiscal de secuestro del aparato y la incautación de datos almacenados en su interior y la autorización judicial respectiva.[53]

No es de extrañar que el dispositivo móvil (celulares, *cell phones*, *smartphone*) se hayan convertido en la estrella de toda investigación judicial en razón de la capacidad de almacenamiento de datos que tienen estos aparatos que han sido considerados con razón como “microprocesadores” que registran una ingente cantidad de información asociada a la vida privada de su usuario y que permiten un grado de injerencia superlativo por parte de terceros y del propio estado.[54]

“Los teléfonos celulares difieren tanto en un sentido cuantitativo como cualitativo de otros objetos que podrían llevarse en la persona de un arrestado. En particular, los teléfonos celulares modernos tienen una inmensa capacidad de almacenamiento. Antes de los teléfonos celulares, la búsqueda de una persona estaba limitada por las realidades físicas y generalmente constituía solo una estrecha intrusión en la privacidad. Pero los teléfonos celulares pueden almacenar millones de páginas de texto, miles de imágenes o cientos de videos. Esto tiene varias consecuencias de privacidad interrelacionadas. Primero, un teléfono celular recopila en un solo lugar muchos tipos distintos de información que revelan mucho más en combinación que cualquier registro aislado. En segundo lugar, la capacidad del teléfono permite que incluso un solo tipo de información transmita mucho más de lo que antes era posible. En tercer lugar, los datos en el teléfono pueden remontarse a años. Además, un elemento de omnipresencia caracteriza a los teléfonos celulares, pero no a los registros físicos. Hace una década, los oficiales podrían haber tropezado ocasionalmente con un artículo muy personal, como un diario, pero hoy en día, muchos de los más del 90% de los adultos estadounidenses que poseen

[51] 573 U.S. 373 (2014).
[52] 728 F.3d 1, 1 (1st Cir. 2013).
[53] Aboso, Gustavo E., “La inconstitucionalidad de la requisa y el examen sin autorización judicial de datos personales almacenados en dispositivos celulares de personas detenidas – Breve reseña de los fallos “Riley vs. California” [573 U.S.132 (2014)] y “United States vs. Brima Wurie” [573 U.S. 212 (2014)] de la Corte Suprema de Justicia de los Estados Unidos”, publicado en la *Biblioteca Jurídica Online elDial.com* el 31/7/2014 [Cita: eldial.com – DC1D2F]. Al respecto, Hairabedian, Maximiliano, “El acceso a información y datos de teléfonos celulares”, *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet*, Daniela Dupuy (dirección), Mariana Kiefer (coordinación), Bdef, Montevideo-Buenos Aires, 2017, pp. 451 y ss.
[54] La incautación de la información almacenada en el dispositivo electrónico sirve en general para acreditar la materialidad del hecho y su gravedad, por ejemplo, en materia de tráfico de sustancias controladas esa información permite corroborar la hipótesis de la acusación pública sobre la comercialización imputada (TSJ Entre Ríos, legajo 2073/23, “Rodríguez, A. A. y Ríos, C. E. s/ comercio de estupefacientes s/ recurso de casación”, sentencia n° 189, de 28/8/2024).

teléfonos celulares mantienen en su persona un registro digital de casi todos los aspectos de sus vidas." [55]

La exigencia de orden judicial también fue requerida en el caso "Trabajo Rueda vs. España"[56] en el que el Tribunal Europeo de Derechos Humanos declaró la violación del artículo 8 de la Convención de Derechos Humanos que tutela el derecho a la privacidad del acusado de poseer material de abuso sexual infantil almacenado en su ordenador que había sido entregado para su reparación. El técnico descubrió de manera casual los archivos de imágenes y vídeos de tal contenido y avisó a la autoridad policial sobre su hallazgo, lo que derivó en una búsqueda rápida de ese contenido para confirmar el hecho y el pedido de secuestro del dispositivo con el objeto de incautar el contenido.

En consecuencia, podemos sostener que la autorización judicial es una condición inevitable cuando nos referimos a la evidencia digital vinculada con la incautación de datos electrónicos.[57]

En el caso de prueba informática, por ejemplo, el secuestro de dispositivos móviles u ordenadores dispuestas en el marco de un proceso por la presunta infracción del artículo 128 del Código Penal, existen reglas de aseguramiento de la prueba que imponen, como primera medida, evitar la eliminación de la prueba inmaterial y efectuar la respectiva copia de respaldo o espejo sobre la cual deberán efectuarse los registros técnicos necesarias que son proporcionadas a las partes del proceso para su debida constatación y peritaje.[58]

Amén de la orden judicial, especial atención merece su fundamentación que debe estar alineada con la naturaleza del objeto procesal para definir su

---

[55] "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person. Notably, modern cell phones have an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.", cfr., *Riley v. California*, pp. 17-21.

[56] Demanda n° 32.600/12, sentencia de 30/5/2017.

[57] Un aspecto distinto se presenta cuando en el régimen de ejecución de la pena se restringe el uso de los celulares en los centros penitenciarios lo que conculca los derechos del condenado al impedir una comunicación permanente con su grupo familiar y así afianzar el régimen de progresividad en el tratamiento punitivo, cfr. STJ Chaco, N° 183, expte. n° 2522/2025-1-C, "Defensoría General Adjunta y Comité contra la Prevención de la Tortura s/ habeas corpus y medida cautelar", de 12/5/2025, en el que se hizo lugar parcialmente a la acción de habeas corpus dirigida contra la Resolución n° 676/22 del Ministerio de Seguridad y Justicia de 23/5/2022 y ley 4033-J sobre la limitación en el uso de celulares e internet en el interior de los establecimientos penitenciarios de la provincia.

[58] CCAPPJCyF, Sala 1, causa n° INC 47207/2019-1, "NN", de 24/11/2020.

necesidad, especialidad o pertinencia y proporcionalidad.[59] El pedido fiscal de incautación de datos almacenados en los dispositivos electrónicos del acusado que debe preceder a la autorización judicial debe establecer el sentido y el alcance del registro con especial referencia al contenido de la evidencia digital, la especificidad de las herramientas digitales aplicadas a la búsqueda de datos y su plazo temporal.[60]

Cuando el plazo temporal de búsqueda excede de manera ostensible la razonabilidad de la medida, la defensa del imputado puede plantear su desproporción en virtud del objeto del proceso y el grado de intensidad de la pesquisa, por ejemplo, se consideró excesivo la fijación de un plazo anual en el registro de las comunicaciones efectuadas por el acusado en el marco de un proceso por tráfico ilegal de estupefacientes.[61]

Un problema adicional y que hemos tratado en otro lugar se relaciona con el acceso a los datos almacenados en el dispositivo y que deben ser incautados para su posterior análisis forense.[62] En términos sencillos existe una extensa discusión sobre la necesidad de una orden judicial para autorizar el uso de la fuerza mínima indispensable para obtener el dato biométrico del acusado. En esta constelación de casos se habla de la obtención compulsiva de los datos de acceso por parte de su titular que resulta imputado en el proceso. En una apretada síntesis hemos concluido que el uso de la fuerza mínima indispensable para la obtención del dato biométrico constituye una inobservancia del principio de incoercibilidad del acusado, es decir, el estado debe respetar su autonomía que se exterioriza en el derecho de resistir la acusación. Nadie puede ser obligado a aportar prueba en su contra, en todo caso le corresponde al acusador público ordenar los medios probatorios que puedan corroborar el objeto del proceso sin necesidad de ejercer coerción sobre el imputado.

En el derecho judicial comparado el Tribunal Supremo español sostuvo la obligatoriedad de la orden judicial para acceder a los datos almacenados en el celular del acusado[63], algo que fue refrendado por la reforma de la ley procesal penal (LO 13/2015) que introdujo en el Título VIII el Capítulo IV titulado “Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos”.

En lo que acá interesa, el artículo 588 bis a) establece los principios rectores entre los que se cuenta el principio de autorización judicial para la adopción de

[59] CCAPPJCyF, Sala 1, causa Nº 17221/2015-4 y 17221/2015-6 “N.N.” (Ley 24762), de 27/09/2017).
[60] CCAPPJCyF, Sala 1, INC n° 26904/2018-1, “R., V. A. s/ art. 128 CP”, de 12/8/2019.
[61] CCAPPJCyF, Sala 3, causa n° 108479/2023-1, “Estrella Quevedo, C. E.”, de 15/12/2023.
[62] Aboso, Gustavo E., *El principio de incoercibilidad del imputado y sus consecuencias en el proceso penal*, 1.ª ed., Albremática, Ciudad Autónoma de Buenos Aires, 2023, pp. 136 y ss.
[63] STS, Sentencia 891/2022, de 11/11/2022.

medidas de investigación vinculadas con evidencia digital, a lo que se agrega la observancia de los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de los registros.

El acceso a los datos almacenados en la agenda del dispositivo electrónico sin orden judicial practicado por la autoridad policial representa una injerencia arbitraria que afecta el derecho a la intimidad, no el del secreto de las comunicaciones.[64]

La ley procesal penal alemana (*Strafprozessordnung*) regula una batería de normas de investigación digital (§§ 100a – 100k StPO) entre las que nos interesa citar en relación con el objeto de nuestro trabajo el § 100i que regula las técnicas de investigación para dispositivos móviles (*Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten*). En particular, este parágrafo establece la posibilidad de aplicar técnicas de geolocalización mediante el uso de mensajes SMS silenciosos.[65]

En esta línea de interpretación, el Tribunal de Justicia de la Unión Europea sostuvo la necesidad del control judicial de los medios de investigación que involucren los datos almacenados en un dispositivo de la persona pesquisada.

"Este control previo requiere que el órgano jurisdiccional o la entidad administrativa independiente encargada de efectuarlo disponga de todas las atribuciones y ofrezca todas las garantías necesarias para conciliar los diferentes intereses legítimos y derechos concurrentes […] por una parte, los intereses legítimos relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de aquellos a cuyos datos afecte el acceso."[66]

El desbloqueo compulsivo de las capas de seguridad del dispositivo electrónico del acusado está íntimamente vinculado con la incautación de datos. Parece existir consenso en torno de que esto último debe ser ordenado por el juez, previo pedido del acusador público, mientras que el desbloqueo de los datos biométricos no parece gozar de la misma aceptación, siendo patente la confusión reinante sobre su procedencia y control.[67]

Así pues se sostiene que la orden judicial de incautación de datos almacenados en el dispositivo electrónico involucra también el acceso a los datos y para esto resulta preponderante determinar si el uso de la violencia mínima sobre el imputado para lograr su colaboración también debería estar autorizada y controlada por el juez.[68]

---

[64] STC, Sentencia 142/2012 de 2/7/2012.
[65] BGH 3 StR 400/17 - Sentencia de 8/2/2018 (KG Berlín); BGH 6 StR 611/21 – Sentencia de 23/3/2022 (LG Magdeburg).
[66] Asunto C-548/21, de 8/10/2024.
[67] Al respecto cfr. voto en minoría del juez Buján en la causa n° 79139/2024-2, "U. A. C. y otros", de 12/6/2025, de la Sala 4 de la Cámara de Casación y Apelaciones del fuero.
[68] Aboso, *El principio de incoercibilidad del imputado...*, pp. 136 y ss.

En un caso se sostuvo que “los agentes de investigación pueden obligar a los sospechosos a poner su huella digital en sus teléfonos inteligentes para acceder a los datos almacenados en ellos. El desbloqueo forzoso puede justificarse en virtud del artículo 81b, párrafo 1, del StPO (Código de Procedimiento Penal alemán), en conjunción con los artículos 94 y siguientes del mismo código, siempre que el acceso posterior previsto a los datos sea proporcionado. Además, el desbloqueo debe servir para facilitar una búsqueda previamente ordenada por un juez en virtud de los artículos 102 y 105, párrafo 1 del StPO, que sirve específicamente para localizar teléfonos móviles. Sin embargo, incluso si la obtención de pruebas fuera ilícita, el BGH no ve fundamento para prohibir su uso.”[69]

Esta sentencia desdobla un hecho único vinculado con la incautación de datos, ya que el desbloqueo compulsivo del dispositivo representa el tramo primario para el acceso a los datos almacenados. En términos más sencillos, sería equiparable a decir que el secuestro de los dispositivos electrónicos ubicados en el domicilio allanado debe ser ordenado judicialmente, pero no es necesario que la orden abarque el ingreso al domicilio.

Una situación extrema está regulada en la ley penal francesa al sancionar como conducta punible el que rehúse aportar un código de encriptación que permita el acceso a los datos almacenados en un dispositivo electrónico vinculado con la comisión de un crimen o delito como una infracción contra la administración de justicia (artículo 434-15-2 de *Code Pénal*).[70]

En el marco de la *enquête pénale*, la ley de procedimientos regula en los artículos 60, 77, 156 y 230-1 a 230-5 del *Code de procédure pénale* la técnica aplicable a los datos almacenados en dispositivos electrónicos en el marco de una investigación judicial. La participación de peritos y la supervisión judicial son las características más sobresalientes del ordenamiento adjetivo galo.

Sobre este tópico podemos señalar que la orden judicial es una condición necesaria y excluyente en la obtención de los datos biométricos y la subsecuente incautación de los datos almacenados en el dispositivo. Acá juegan de manera coordinada dos principios rectores en la materia, por un lado, la orden judicial para obtener de manera compulsiva el registro biométrico que permite el acceso a los datos cuya incautación se ordena se vincula directamente con el principio de incoercibilidad del acusado. Semejante medida judicial importa la afectación lisa y llana del derecho del acusado de no colaborar con la investigación judicial (*nemo tenetur ipse procedere*). Autorizar el uso de la fuerza mínima por parte de la autoridad policial o de funcionarios judiciales significa una inobservancia de los principios de autonomía, libertad y dignidad del acusado.

En todo caso, antes de ordenar la obtención compulsiva de los datos biométricos se debería proceder a la implementación de los programas informáticos especialmente diseñados para sortear los factores de seguridad

[69] BGH, Sentencia 2 StR 232/24, de 13/5/2025.
[70] Cour de cassation, Assemblée plénière, de 7/11/2022, n° 21-83.146; Cour cassation, Chambre criminelle, de 6/3/2024, n° 23-81.132.

del sistema. Recién ahí uno podría empezar a cuestionar la necesidad de la colaboración extorcada del imputado. También nos hemos referido a este tema en otro espacio, pero no es ocioso recordar que el dato biométrico es uno de naturaleza personal alcanzado por la ley de protección de datos y que representa la llave para el ingreso a los contenidos almacenados en el aparato.[71]

La doctrina judicial nacional parte de la base de que cualquier tipo de injerencia en el ámbito de la privacidad de las comunicaciones o la incautación de datos almacenados en dispositivos electrónicos del acusado debe estar autorizada judicialmente. En el contexto de la evidencia digital, por ejemplo, se anuló los pedidos de informes cursados por el acusador público sobre datos electrónicos asociados al uso del celular del acusado con el objeto de establecer mediante geolocalización su ubicación en un período de tiempo determinado[72], haciéndola extensible a los datos personales relacionados con el uso del transporte público mediante el almacenamiento de datos vinculados a la tarjeta empleada por el acusado en el sistema de registro público (Sistema Único de Boleto Único o "SUBE").[73]

No resulta ocioso recordar que el Tribunal de Justicia de la Unión Europea sostuvo que:

"En lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos pretendido por la normativa controvertida, de conformidad con el principio de proporcionalidad, el Tribunal de Justicia considera que solo los objetivos de lucha contra la delincuencia grave o de prevención de las amenazas graves contra la seguridad pública pueden justificar el acceso de las autoridades públicas a un conjunto de datos de tráfico o de localización que puedan permitir extraer conclusiones precisas sobre la vida privada de las personas afectadas, sin que otros factores relativos a la proporcionalidad de la solicitud de acceso, como la duración del período para el que se solicita el acceso a dichos datos, puedan conllevar que el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general justifique tal acceso."[74]

La dificultad conceptual y técnica que conlleva implícitamente la regulación y el tratamiento de la evidencia digital en el ámbito de la administración de justicia

---

[71] Aboso, Gustavo E., "Desbloqueo coactivo de datos biométricos y «nemo tenetur se ipsum accusare»", en *Sistema Penal e informática*, Volumen 6 . Ciberdelitos. Evidencia Digital. Tics, Marcelo Riquert (Director) y Carlos Christian Sueiro (Coordinador), Hammurabi, 2023, pp. 276 y ss.

[72] El pedido de informes sobre los registros de geolocalización de una persona sospechada de haber participado en varios robos en una zona determinada de la ciudad mediando orden judicial fue considerada como un registro arbitrario por carecer de causa probable para legitimar el pedido a la luz de la Cuarta Enmienda de la Constitución de los Estados Unidos, cfr. *Carpenter v. United States*, 819 F. 3d 880. Entre nosotros, TSJ CABA, por mayoría, Expte. n° QTS 81922/2021-3, "Ministerio Público – Fiscalía de Cámara Norte de la CABA s/ Queja por recurso de inconstitucionalidad denegado en Callata, Mauro Ezequiel s/ 149 bis Amenazas", de 13/12/2023.

[73] CCAPPJCyF, Sala I, causa n° 561768/2022, "C., M. E.", de 22/3/2022.

[74] Sentencia en el asunto C-746/18, "H. K/Prokuratuur", Comunicado de Prensa n° 29/21, de 2/3/2021.

no es algo nuevo, todo lo contrario, el uso de herramientas forenses de naturaleza digital obliga a los órganos judiciales a reconsiderar aspectos novedosos e inéditos sobre el sentido y el alcance de la evidencia digital de cara a la garantía del debido proceso y el aseguramiento de la defensa en juicio. Con especial énfasis se ha señalado que el uso de la tecnología en la investigación penal ofrece distintos puntos de vista controvertidos en relación con la defensa material en juicio y el principio de igualdad de armas.[75]

Hace poco tiempo el Tribunal Europeo de Derechos Humanos subrayó la relación de tensión que existe con el uso de las nuevas tecnologías en el procedimiento penal y las limitaciones que encuentra el acusado y su defensa técnica para afrontar este nuevo desafío, de modo singular cuando la prueba de cargo está íntegramente constituida por evidencia digital, en el caso concreto se trató el uso de un sistema de mensajería instantánea (*ByLock*), cuyo uso quedó descontinuado ante la denuncia del gobierno turco de que sus usuarios eran integrantes de grupos terroristas y la aplicación era empleada para coordinar atentados criminales. La detención de su creador y administrador por parte de la autoridad turca y la condena impuesta bajo el imperio de las leyes antiterroristas desataron una auténtica cacería de brujas que abarcó a un sinnúmero de usuarios que no tenían vinculación alguna con la organización criminal.[76]

En este proceso se corroboró que la defensa del acusado no tuvo oportunidad procesal de acceder a la información obtenida por el gobierno a partir de la incautación de datos obtenidos del sistema de mensajería cuestionado, sumado a una serie de restricciones que hicieron imposible ejercer una defensa adecuada para contrarrestar la acusación de pertenencia a una organización criminal, delito por el cual fue condenado.

El meollo de la discutida cuestión de la evidencia digital se agrava cuando el contenido de los tipos de injusto penal doloso está integrados por datos o archivos electrónicos que constituyen el objeto de las acciones incriminadas. Por ejemplo, en los delitos de tenencia, difusión y distribución de material de abuso sexual infantil el objeto de las acciones descritas recae sobre un elemento informático que ocupa en la actualidad el centro de la escena de la prevención y la represión de estos comportamientos vinculados a la política criminal internacional enfocada en la prevención y el castigo de los abusos y explotación sexuales de los infantes. Por lo tanto, la evidencia digital en esta hipótesis normativa ya viene preconfigurada en atención a los avances tecnológicos en la creación de material sintético y el anonimato que asegura el acceso a las redes telemáticas.

Por lo tanto, parece previsible que la relación asimétrica que siempre existe en el proceso penal entre el acusador público y el imputado asistido por la defensa

[75] Sieber, Ulrich, *Gutachten C zum 69. Deutschen Juristentag. Straftaten und Strafverfolgung im Internet*, C. H. Beck, München, 2012, C 103 y ss.; C 112 y ss.; C 155 y ss.
[76] ECHR, *Yüksel Yalçinkaya v. Türkiye*, n° 15.669/20, de 26/9/2023, párr. 302 y ss., párr. 312 y ss. Existen otras demandas resueltas de manera favorable para los accionantes por las mismas circunstancias, cfr. ECHR, *Çolakoğlu v. Türkiye*, n° 13.762/20, de 19/2/2021, entre otros.

técnica se intensifique a la luz de la creación de unidades fiscales especializadas que cuentan con una mayor proporción de recursos humanos y técnicos que ocluyen la posibilidad de la igualdad de armas atento que ni siquiera la defensa pública cuenta con el presupuesto dinerario para hacer frente a la continua y creciente demanda que requiere la evidencia digital.

Tampoco cabe acudir a la doctrina de la "Plain View"[77] para justificar el hallazgo de material incriminante almacenado en el dispositivo electrónico del acusado cuando el objeto del proceso en el que se libró la respectiva orden de incautación de datos no estaba mínimamente vinculada con la naturaleza del delito investigado.[78]

Nuevamente acá huelga reiterar que el pedido de informes a cualquier organismo o instituto público o privado que tenga a su cargo la administración de una base de datos personales debe estar precedido por la debida orden judicial, *in fortiori*, si se trata de una persona imputada de delito o contravención.

Una situación de excepción se presenta cuando el titular de los datos presta su consentimiento informado para el acceso y posterior incautación con el objeto de ser peritado. El consentimiento informado requiere que el afectado haya sido informado de sus derechos judiciales, entre ellos, el de negarse a cooperar con la investigación judicial. La presencia de su abogado de confianza durante el procedimiento y el suministro de las claves de acceso a los dispositivos electrónicos en poder del acusado y que fueran secuestrados para su posterior peritaje ha sido declarado válido.[79]

Consecuencia jurídica de la falta de notificación al acusado y la frustración de su participación en la pericia digital

En términos generales, las leyes procesales que se basan en el sistema acusatorio establecen que el fiscal deberá notificar a las partes, imputado y víctima respectivamente, sobre la realización de la pericia, los puntos salientes y la posibilidad de ejercer el debido control sobre la prueba mediante la designación de peritos de parte. A su vez, la participación de la defensa del acusado es necesaria para resguardar el debido proceso legal y el derecho de defensa en juicio. El incumplimiento de la notificación acarrea la nulidad de lo actuado, aunque eso dependerá también de la normativa aplicable, ya que no todos los regímenes procesales establecen la nulidad del acto como consecuencia de la inobservancia de tal deber.

En el caso de la ley procesal penal local, el Capítulo 7 del Libro Primero regula la nulidad de los actos procesales y, en especial, el artículo 77 establece la regla general para la declaración de nulidad de los actos procesales, mientras

[77] *Horton v. California*, 496 U.S. 128 (1990).
[78] CCAPPJCyF, Sala I, causa n° 12141374/2018, "D., F. R.R.", de 26/9/2018.
[79] STS, Sala de lo Penal, 2205/2019, de 27/6/2019.

que el artículo 78 regula la nulidad genérica, entre otras, cuando se hubiera omitido la intervención de la defensa.[80]

Más allá de la regulación específica sobre la materia probatoria, lo cierto es que la declaración de nulidad del acto pericial puede ser relativizada a partir de considerar que el acto es reproducible, en cuyo caso pesa sobre la defensa solicitar la renovación de la prueba, proponer puntos de pericia que no hayan sido ya contestados y, por último, plantear las objeciones que crea conveniente a través del informe practicado por el profesional designado a tal efecto.

En cambio, cuando la pericia resulta irreproducible[81], entonces sí corresponde declarar la nulidad de la experticia por falta de control de la defensa, pero en cualquier caso deberá acreditarse cuál es el perjuicio que le acarrea la falta de control de la defensa a través del perito de parte, ya que la nulidad por la nulidad misma no integra el sistema procesal vigente.

La pretensión de falsedad o alteración de las conversaciones mantenidas entre el imputado y la presunta víctima mediante el sistema de mensajería instantánea no justifica su expulsión del proceso como prueba de cargo si la defensa no asume el compromiso de demostrar que ese contenido impugnado era falso o que se utilizó una aplicación que permite la generación de falsos contenidos. Por lo demás, su autenticidad puede ser demostrada mediante otros medios de prueba existentes en el procedimiento.[82]

De la prueba digital vinculada con las comunicaciones intercambiadas entre el acusado y su presunta víctima mediante el sistema de mensajería instantánea se ha dicho que debe obrarse con cautela frente a este tipo de evidencia, ya que el anonimato y la posibilidad técnica de crear cuentas falsas abre un abanico de posibilidades al fraude procesal.[83]

El Tribunal Supremo de Justicia español sostuvo que:

“Respecto a la queja sobre la falta de autenticidad del diálogo mantenido por Ana María con Constancio a través del Tuenti, la Sala quiere puntualizar una idea básica. Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa

[80] Aboso, *Código Procesal Penal de la Ciudad Autónoma de* Buenos, pp. 128 y ss.
[81] Aboso, *ob. cit.*, comentario del artículo 105.
[82] STS, Sala de lo Penal, 634/2025, de 13/2/2025.
[83] STS, Sala de lo Penal, 3292/2025, de 1/7/2025; 5421/2015, de 27/11/2025.

comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido."[84]

Sin embargo, también se reconoce que lo dubitable de la prueba digital basada en impresiones de pantallas de las conversaciones o demás comunicaciones obtenidas del celular de la víctima que fueran entregadas de manera voluntaria, aunado al testimonio de terceras personas sobre su veracidad, habilitan al tribunal a su ponderación positiva para acreditar el hecho denunciado, en especial, cuando estamos frente a delitos sexuales en contra de menores de edad.[85]

En un proceso sustanciado en contra de una persona acusada de haber amenazado en repetidas ocasiones a su expareja mediante el sistema de mensajería instantánea ("We Chat"), ella aportó distintas impresiones del contenido de los mensajes intimidatorios enviados por el imputado y si bien la ponderación de este material como elemento probatorio puede ser relativizado cuando no ha sido confirmada su autenticidad mediante la debida pericia informática, el reconocimiento expreso del autor de los mensajes, aunque restando importancia a su contenido, permite su valoración como elemento de cargo.[86]

Corolario

La distinción entre extracción e incautación de datos electrónicos mediante una pericia forense está enfocada en el sujeto procesal y el acuerdo prestado para su acceso. En el caso de la víctima, por lo general, no se requiere orden judicial cuando ella aporta de manera voluntaria los registros de las comunicaciones bidireccionales almacenadas en su dispositivo electrónico. No constituye una afectación a la privacidad el acceso a los datos de tráfico almacenados en el celular de la víctima cuando ella los aporta de manera voluntaria con el objeto de acreditar los extremos de su denuncia.

Tampoco acá el acusado puede invocar una violación del secreto de las comunicaciones o de su intimidad cuando la comunicación puede revestir relevancia típica. Por lo tanto, el concepto de "extracción" hace honor a la puesta a disposición de la autoridad el contenido de datos electrónicos que permiten recrear los hechos desde la perspectiva de la prueba digital.

En cambio, cabe hacer una distinción sobre la procedencia de la prueba digital cuando la víctima presenta en el proceso fotos de pantalla o cualquier otro dato de interés sin mediar la intervención de los profesionales informáticos que permitan asegurar su autenticidad. Si bien los documentos introducidos en el curso de la investigación pueden ser meramente indiciarios y el acusado puede

[84] STS, Sala de lo Penal, 191/2023, de 19/1/2023 y 191/2023, de 1/7/2025.
[85] STS, Sala de lo Penal, 300/2015, de 19/5/2015. En este proceso se valoró positivamente el contenido de los mensajes intercambiados entre la víctima menor de edad y su compañero de colegio sobre los abusos sexuales sufridos en manos de la pareja de su madre para corroborar la credibilidad de aquélla.
[86] STS, Sala de lo Penal, 754/2015, de 27/11/2015.

impugnar su introducción o correcta ponderación, si confluyen otros medios de prueba que permitan disipar la duda inicial nada obsta para que puedan ser valorados entre el conjunto del plexo probatorio que sustenta la acusación pública, privada o ambas.

La situación es la opuesta cuando se trata de la incautación de datos de fuentes digitales en poder del acusado. Acá la orden judicial es indispensable. Por lo demás, la intensidad de la injerencia en el ámbito de la vida privada del imputado dependerá en gran medida del contenido de lo injusto típico del delito o delitos investigados. También el grado de intromisión debe guardar relación de proporcionalidad en razón de las circunstancias espaciotemporales en las que se ejecutó el hecho o los hechos objetos del proceso. Sobre esta situación le corresponde al acusador público establecer en el decreto de determinación de los hechos cuál es el objeto del proceso, justificar la necesidad del secuestro de los dispositivos y la posterior incautación de datos electrónicos, seguido de la especificidad sobre los programas a utilizarse y el rango de búsqueda en un primer momento mediante el triaje. La circunstancia temporal es importante, ya que cuanto más se retrotraiga en el tiempo el registro mayor será la necesidad de fundamentar esta clase de injerencia.

Por último, la delimitación tradicional de informe de pericia forense aplicada comúnmente por nuestros tribunales no resulta eficaz para la evidencia digital, puesto que se da por descontado que cualquier forma de extracción o incautación de datos debe estar precedida por la intervención de un profesional o especialista en la materia, sumado a que las herramientas forenses que se utilizan a tal efecto demuestran de manera acabada, según los protocolos vigentes de investigación judicial, que la comprobación y la conservación de los datos de interés para el proceso no resulta de un simple proceso visual o técnico, sino que demanda un conjunto de protocolos que involucran el tratamiento de datos almacenados en el dispositivo del acusado.

En consecuencia, la posibilidad de fiscalización a través de un perito de parte constituye un derecho esencial en el ejercicio competente de la defensa en juicio como corolario obligado de la garantía del debido proceso. Pero también debe dejarse aclarado que cuando se tratare de prueba reproducible, el imputado tiene el derecho de ofrecer puntos de pericia o cuestionar el informe forense de los especialistas, pero si no lo hace en tiempo y forma ello no acarrea de modo inevitable la nulidad del acto procesal.

Citar: elDial DC36E6