SECUESTRO DEL CELULAR Y ACCESO AL CONTENIDO EN EL PROCESO PENAL ARGENTINO

Alcance de la orden, código de desbloqueo, biometría y autoincriminación

Trabajo doctrinario para ST Abogados - sección Artículos

Dr. Jacobo Iván Selser

Buenos Aires, 2026

Tesis de lectura. Secuestrar un teléfono y acceder a su contenido son actos distintos. El primero recae sobre un objeto; el segundo, sobre comunicaciones, archivos, ubicación, vínculos y datos íntimos. Por eso, el acceso al contenido no debe presumirse cubierto sin más por la incautación del aparato: exige una habilitación fundada, un objeto definido, una delimitación razonable y posibilidad real de control por la defensa.

Versión final revisada. Se depuraron las afirmaciones categóricas, se separaron jurisdicciones y se trataron como controvertidos los puntos que todavía no tienen una regla nacional uniforme, en especial el desbloqueo biométrico compulsivo.

Resumen ejecutivo

El secuestro de teléfonos celulares aparece hoy en allanamientos, requisas, detenciones y medidas urgentes de investigación. La práctica, sin embargo, suele tratar como un solo acto lo que jurídicamente conviene distinguir: incautar el aparato, acceder a su contenido y examinar técnicamente los datos obtenidos. Esa distinción ordena el problema y evita dos errores simétricos: asumir que todo acceso es inválido o entender que el secuestro físico habilita una exploración completa de la vida digital.

El teléfono actual no contiene sólo un posible mensaje relacionado con el hecho investigado. Puede reunir años de comunicaciones, fotografías, geolocalización, credenciales de aplicaciones, información bancaria, datos de salud, archivos laborales y conversaciones de terceros ajenos al proceso. Por eso, el ingreso al contenido exige una justificación más precisa que la mera utilidad investigativa: finalidad concreta, alcance definido, proporcionalidad, preservación técnica y control de la defensa.

El problema del código de desbloqueo muestra esa tensión con particular claridad. Pedir un PIN, un patrón o una contraseña implica requerir un aporte cognitivo: la persona debe recordar y comunicar un dato para facilitar una prueba que puede perjudicarla. Allí la garantía contra la autoincriminación opera con fuerza. La biometría -huella, rostro, iris- plantea una discusión distinta: algunos tribunales la asimilan a una prestación corporal tolerable bajo control de proporcionalidad; otros advierten que forzar el cuerpo para abrir la vida digital compromete intimidad, dignidad e incoercibilidad. No hay una regla nacional uniforme.

La conclusión práctica es de método. La defensa debe auditar el puente entre el objeto secuestrado y el dato usado en la acusación. La querella y la fiscalía deben pedir medidas acotadas, documentar la preservación y evitar accesos informales. La solidez de la prueba digital no depende sólo de lo que aparece en pantalla, sino de la legalidad del acceso, la trazabilidad del procedimiento y la posibilidad real de contradicción.

Índice de lectura

1. El problema: por qué el celular no es un objeto más

Durante mucho tiempo el proceso penal trató al teléfono como una cosa entre otras. Se lo secuestraba, se lo inventariaba y se lo describía como quien describe un arma, una agenda o un sobre. Esa lógica quedó corta. Un smartphone actual puede concentrar una porción extensa de la biografía digital de una persona y, además, datos de terceros que no son investigados.

De allí surge una consecuencia jurídica concreta. El interés estatal en investigar no desaparece, pero cambia la escala del derecho afectado. Abrir un teléfono se parece menos a abrir un objeto y más a ingresar a un ámbito de privacidad compuesto por comunicaciones, ubicaciones, fotografías, archivos, aplicaciones y rastros de

comportamiento. Si un domicilio no se allana con fórmulas genéricas, la vida digital tampoco debería quedar expuesta por inercia.

El punto de partida no es preguntar si el contenido del celular puede servir como prueba. Puede servir. La pregunta anterior es bajo qué condiciones se accedió a ese contenido, con qué límite, por quién, con qué método y bajo qué posibilidad de control. Si el ingreso fue ilegítimo o desproporcionado, la discusión sobre valor probatorio llega tarde.

2. Tres actos que conviene no confundir: secuestro, acceso y examen

La práctica suele tratar como un bloque lo que en rigor son tres momentos separables. Distinguirlos es la herramienta analítica principal para litigar este tema.

El primer momento es el secuestro físico del aparato. Recae sobre el dispositivo como cosa: identificación, marca, modelo, IMEI, SIM, estado de encendido o bloqueo, embalaje, inventario, lacrado, traslado y custodia. Hasta allí no se ha leído nada; sólo se aseguró el objeto.

El segundo momento es el acceso al contenido. Encender, desbloquear, navegar, copiar bases de datos, leer chats o entrar a cuentas asociadas son actos que recaen sobre datos, comunicaciones y registros íntimos. Ese paso no debería presumirse cubierto sin más por el secuestro del aparato: debe verificarse qué habilitó la orden, cuál era el objeto de la búsqueda y hasta dónde podía llegar.

El tercer momento es el examen técnico o pericial. Allí importan la metodología de extracción, la herramienta usada, la versión del software, la copia de trabajo, el cálculo de integridad, el análisis de metadatos, el reporte y la posibilidad de que la defensa controle o replique el procedimiento.

Existe, además, una tensión jurisprudencial que conviene no ocultar. Cierta jurisprudencia nacional entendió que copiar datos de un teléfono ya incautado no constituye, por sí, una pericia. La lectura más protectora responde que la discusión no se agota en la etiqueta del acto -pericia o diligencia investigativa-, sino en la cobertura constitucional y procesal del acceso. Esa tensión explica por qué el planteo debe formularse con precisión.

Acto	Sobre qué recae	Qué exige	Riesgo principal
Secuestro físico	El dispositivo como objeto.	Identificación, IMEI, estado, embalaje, inventario y custodia.	Defectos de acta o cadena física.
Acceso al contenido	Comunicaciones, archivos, cuentas y datos íntimos.	Habilitación fundada, finalidad concreta y alcance delimitado.	Ingreso sin cobertura suficiente o exploración general.
Examen técnico	La lectura y procesamiento de lo accedido.	Método documentado, integridad, trazabilidad y control de partes.	Reporte opaco, falta de hash o ausencia de contradicción.

3. Marco constitucional: intimidad, comunicaciones y autoincriminación

El análisis arranca en los artículos 18 y 19 de la Constitución Nacional. El artículo 18 protege la defensa en juicio, el debido proceso, la inviolabilidad de ámbitos especialmente resguardados y la garantía de no ser obligado a declarar contra sí mismo. El artículo 19 preserva un ámbito de reserva que no puede ser invadido sin una razón constitucionalmente suficiente. Sobre un teléfono celular, ambos planos operan de manera simultánea.

La Corte Suprema fijó estándares que se proyectan sobre la prueba digital. En Halabi, al examinar comunicaciones telefónicas e internet, rechazó esquemas amplios de captación sin determinación suficiente de supuestos y justificativos. En Quaranta, al tratar una intervención telefónica, sostuvo que una medida dirigida a

conocer el contenido de comunicaciones sólo puede disponerse con elementos objetivos que funden una sospecha razonable; una fórmula vaga o un llamado anónimo, por sí solos, no sustituyen la motivación judicial.

La garantía contra la autoincriminación agrega una capa específica. Su núcleo protege a la persona frente a la exigencia de realizar un acto propio, voluntario y cognitivo que produzca prueba en su contra. Esa es la clave para diferenciar el PIN o patrón de desbloqueo, que la persona conoce, de ciertos datos corporales o biométricos, cuya utilización compulsiva abre otra discusión constitucional.

4. Marco procesal argentino: CPPF, CPPN y Provincia de Buenos Aires

4.1. Código Procesal Penal Federal

El CPPF ofrece la formulación más clara para evidencia digital. El art. 151 regula la incautación de datos: por auto fundado y a requerimiento de parte, el juez puede ordenar el registro de un sistema informático o de un medio de almacenamiento para secuestrar componentes, obtener copia o preservar datos de interés. La regla no convierte al teléfono en un territorio sin límites; remite a las restricciones propias del secuestro de documentos y a la preservación de la cadena de custodia.

El art. 152 regula la apertura y examen de correspondencia y objetos; el art. 156 ordena la custodia y devolución de efectos secuestrados; y el art. 157 establece la cadena de custodia para asegurar identidad, estado y conservación de los elementos de prueba, identificando a quienes tomaron contacto con ellos. Leídas en conjunto, estas reglas confirman que obtener datos de un sistema o medio de almacenamiento exige fundamento y trazabilidad.

4.2. CPPN y Provincia de Buenos Aires

El CPPN clásico no tiene una arquitectura tecnológica equivalente. Allí la cuestión se trabaja con categorías tradicionales adaptadas al soporte digital: allanamiento, registro, secuestro, custodia, conservación y pericia cuando para conocer o valorar un hecho hacen falta conocimientos especiales, conforme al art. 253. En ese marco, el control pasa por la motivación de la orden, el alcance del secuestro, la forma de apertura, la necesidad de conocimiento técnico y el derecho de contradicción.

En la Provincia de Buenos Aires, la Ley 11.922 también obliga a discutir reglas de registro, allanamiento, secuestro, comunicaciones por cualquier medio y pericia, junto con los protocolos de cadena de custodia que correspondan. La cautela editorial y litigiosa es no mezclar jurisdicciones: el régimen federal, el CPPN, la Ciudad y la Provincia no son idénticos, y un precedente de una jurisdicción no opera automáticamente como regla de otra.

4.3. Protocolos técnicos

En el plano técnico-oficial, la Resolución 232/2023 del Ministerio de Seguridad aprobó el Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital. No reemplaza al código procesal ni a la orden judicial, pero sirve como parámetro para evaluar buenas y malas prácticas de preservación. Los estándares NIST sobre informática forense móvil tampoco son derecho argentino; sí ofrecen soporte técnico para explicar por qué no es lo mismo mirar, exportar, copiar o adquirir forensicamente un contenido.

5. El código que se sabe: PIN, patrón y contraseña

La discusión es más nítida cuando se trata del PIN, el patrón o la contraseña. Pedirle a una persona que los revele es exigirle un acto positivo, voluntario y cognitivo: debe recordar una información y comunicarla para que el Estado pueda acceder a datos que podrían incriminarla. Esa exigencia roza el núcleo de la garantía contra la autoincriminación.

La Cámara Federal de Casación Penal, en C., R. E., reconoció que los datos contenidos en un celular integran un ámbito de intimidad y privacidad, y que no puede agravarse la situación del imputado por no haber facilitado el código de acceso. La consecuencia no es que toda evidencia del teléfono sea inválida; es más precisa: el Estado no puede convertir la falta de colaboración en indicio de culpabilidad ni desplazar sobre el imputado el deber de abrir el dispositivo.

La causa Ríos, tramitada en la jurisdicción federal de Salta, refuerza esa línea en un escenario específico: se cuestionó la forma en que se había obtenido el patrón de desbloqueo y se rechazó la explotación de un equipo, con posterior rechazo de la queja fiscal por la Cámara Federal de Salta. La enseñanza prudente no es convertir el caso en regla absoluta, sino tomarlo como advertencia: el acceso a la información de un celular requiere cobertura judicial y no puede descansar en una cooperación obtenida sin resguardos suficientes.

6. La biometría: lo que la persona es, y un debate abierto

La huella dactilar, el rostro y el iris plantean un problema distinto. A diferencia del PIN, no son algo que la persona recuerda y comunica, sino rasgos físicos. Esa diferencia -entre saber y ser- explica la división jurisprudencial.

Una línea admite el desbloqueo biométrico compulsivo. Lo asimila a una injerencia corporal no degradante, comparable a tomar impresiones dactilares, imágenes o muestras, en la que el imputado actuaría como objeto de prueba y no como fuente de una declaración. Para esta posición, la medida puede ser válida si supera un test de proporcionalidad: idoneidad, necesidad, razonabilidad, mínima fuerza, orden fundada y alcance acotado. El caso Mora, de la Cámara Federal de Bahía Blanca, suele citarse como ejemplo de esta postura.

Otra línea lo rechaza o lo mira con mayor sospecha. Sostiene que forzar el uso del cuerpo para abrir una vida digital entera no es una simple constatación corporal, sino una utilización coactiva de la persona como instrumento para producir prueba de cargo. En la justicia de la Ciudad, la discusión aparece en resoluciones recientes sobre reconocimiento facial, iris o huella, con votos que ubican la medida dentro del principio de incoercibilidad.

No hay, a la fecha, una regla nacional uniforme. Lo jurídicamente correcto es presentar la biometría como un punto controvertido, sensible a la jurisdicción, al grado de coerción, al objeto de la búsqueda, a la existencia de medios menos lesivos y a la fundamentación concreta de la orden. Quien afirme que el tema está cerrado, en cualquier sentido, simplifica en exceso.

Naturaleza	Ejemplos	Garantía en juego	Estado jurisprudencial
Algo que la persona sabe	PIN, patrón, contraseña.	No autoincriminación: exige aporte cognitivo y voluntario.	Línea fuerte: no puede compelirse ni valorarse en contra la negativa.
Algo que la persona es	Huella, rostro, iris.	Intimidad, incoercibilidad y proporcionalidad.	Debate abierto: una línea lo admite bajo control estricto; otra lo rechaza.

7. Alcance de la orden y pesca probatoria digital

Aun cuando exista cobertura para acceder, queda la pregunta decisiva: hasta dónde. Una orden que autoriza revisar todo el teléfono, sin recorte temporal ni objetivo, se aproxima a una exploración general de la vida digital. El riesgo no es sólo defensivo. También debilita la prueba, porque una medida desproporcionada o imprecisa es más vulnerable al contradictorio.

La jurisprudencia de la Ciudad avanzó en esta dirección. En Villalba Cuyari se remarcó la necesidad de delimitar la pericia sobre el celular, en especial temporalmente. No es lo mismo buscar comunicaciones de una ventana de fechas vinculada al hecho que volcar años de actividad sin criterio. La delimitación protege intimidad del titular y de terceros, y a la vez vuelve más robusta la prueba útil.

La buena orden debería indicar qué se busca, en qué período, en qué aplicaciones o tipos de datos, con qué palabras clave si corresponde, y cuál es la relación entre ese universo de búsqueda y el hecho investigado. Cuanto más se parece a una búsqueda focalizada y menos a una expedición, mejor resiste el control.

8. Apertura sin orden, urgencia y consentimiento

Tres escenarios concentran problemas. El primero es la apertura policial del teléfono en el lugar del procedimiento, sin orden y sin urgencia real. Encender, desbloquear, navegar o fotografiar contenido antes de la intervención técnica puede generar dos objeciones: falta de cobertura para el acceso y afectación de la integridad o trazabilidad de lo que luego se perita.

El segundo escenario es la urgencia. Existen casos en los que la demora puede frustrar la prueba: riesgo de borrado remoto, sincronización, pérdida de sesión o modificación del estado del equipo. Pero la urgencia debe ser explicada y documentada. Preservar no es explorar. Aislar el dispositivo de la red, impedir una alteración o resguardar su estado es distinto de leer su contenido.

El tercer escenario es el consentimiento. Una entrega voluntaria por parte de una víctima o testigo puede tener relevancia. También puede existir una autorización de acceso prestada por una persona investigada. Pero la voluntariedad no se presume: deben analizarse información previa, contexto, detención, presión, alcance de lo autorizado y posibilidad real de comprender las consecuencias.

9. Problemas litigiosos típicos

Secuestro válido, acceso dudoso. El aparato fue incautado correctamente, pero se ingresó al contenido sin orden suficiente o excediendo su alcance.

Orden genérica. La autorización permite revisar todo el teléfono sin recorte temporal, material o aplicativo. La defensa debe discutir proporcionalidad; la acusación debe justificar o acotar.

Exigencia del PIN o patrón. Cuando se pretende derivar un indicio de la negativa a aportar la clave, aparece un choque directo con la garantía contra la autoincriminación.

Desbloqueo biométrico compulsivo. El uso forzado de huella, rostro o iris está discutido. El resultado depende de la jurisdicción, del grado de coerción y del test de proporcionalidad.

Apertura manual previa a la pericia. Si alguien encendió, navegó o capturó contenido antes del trabajo técnico, debe reconstruirse quién, cuándo, cómo y con qué cobertura.

Datos de terceros. El teléfono expone conversaciones y archivos de personas ajenas al proceso. Un acceso amplio puede afectar su intimidad y debilitar la medida.

Confusión entre nulidad y peso probatorio. No todo defecto produce exclusión. Algunos vicios afectan licitud; otros reducen fuerza probatoria; otros exigen demostrar perjuicio concreto.

10. Estrategia para la defensa

La defensa no debería limitarse a negar el contenido. Su trabajo es auditar el puente que va del aparato al dato y del dato a la persona, ubicando con precisión dónde se produjo el quiebre. La pregunta no es sólo si el chat, foto o archivo existe, sino si el Estado podía acceder a él, con qué alcance y bajo qué control.

- Orden: si autorizaba sólo el secuestro del objeto o también el acceso a datos, copia, búsqueda y pericia.
- Acta de secuestro: hora, lugar, funcionarios, testigos, marca, modelo, IMEI, SIM, estado de bloqueo y embalaje.
- Acceso: si hubo apertura, encendido, navegación o captura previa a la pericia, y con qué cobertura.
- Clave: si se exigió el PIN o patrón, o si se valoró en contra la negativa a aportarlo.

- Biometría: si hubo desbloqueo compulsivo, qué orden lo fundó y qué proporcionalidad se explicó.
- Cadena de custodia: del dispositivo y del archivo, con identificación de quienes tomaron contacto.
- Método y herramienta: tipo de extracción, software, versión, operador, hash y límites de búsqueda.
- Control: notificación a la defensa, posibilidad de consultor técnico y acceso al informe completo.
- Alcance: si la búsqueda fue temporal y objetivamente acotada o una exploración general.
- Consecuencia: distinguir ilicitud y exclusión, nulidad con perjuicio, o mera discusión de peso probatorio.

La precisión es decisiva. Un acceso al contenido sin cobertura suficiente puede plantearse como ilicitud y exclusión. Una ruptura grave de cadena, con perjuicio concreto, puede fundar nulidad. Un defecto menor o una explicación técnica insuficiente tal vez deba discutirse como debilidad probatoria. No todo vicio tiene la misma consecuencia.

11. Estrategia para querella y acusación

La acusación que se apoya en un acceso amplio y poco documentado deja flancos previsibles. La que preserva el dispositivo, pide cobertura adecuada y acota la búsqueda construye una prueba más resistente. En evidencia digital, la prolijidad inicial suele valer tanto como el contenido hallado.

- Asegurar y aislar el dispositivo para evitar borrado remoto o sincronización, sin explorar su contenido.
- Solicitar una orden que cubra expresamente el acceso a datos, y no sólo el secuestro del objeto.
- Delimitar la búsqueda por franja temporal, aplicaciones, tipos de datos o palabras clave vinculadas al hecho.
- Obtener el acceso por vías técnicas, sin trasladar al imputado el deber de aportar la clave.
- Documentar la voluntariedad cuando el material es entregado por víctima o testigo.
- Pedir extracción forense cuando se discutirán autenticidad, integridad, autoría o contexto.
- Preservar cadena de custodia del aparato y del archivo, con trazabilidad y valores de integridad cuando corresponda.
- Resguardar la intimidad de terceros y separar lo relevante de lo ajeno al proceso.
- Explicar al tribunal cómo cada paso técnico se relaciona con el hecho imputado.

12. Jurisprudencia de referencia

La selección siguiente prioriza precedentes verificables y se ofrece con cautelas de uso. Algunos no tratan teléfonos celulares en sentido estricto y se citan por su estándar constitucional; otros pertenecen a la justicia de la Ciudad o a tribunales federales específicos y no constituyen una regla nacional automática.

CSJN, Halabi, Fallos 332:111 (2009). Estándar de privacidad y comunicaciones. Rechaza esquemas amplios de captación sin supuestos y justificativos suficientes. No es un fallo sobre desbloqueo de celulares.

CSJN, Quaranta, Fallos 333:1674 (2010). Intervención telefónica inmotivada. Exige elementos objetivos idóneos para una mínima sospecha razonable. Se proyecta por analogía sobre órdenes genéricas de acceso digital.

CFCP, Sala I, C., R. E., Reg. 27/20 (2020). Reconoce el ámbito de intimidad del celular y rechaza agravar la situación por no facilitar el código de acceso. No excluye automáticamente toda evidencia del teléfono.

Ríos, FSA 6443/2023/2, jurisdicción federal Salta. El incidente exhibe la necesidad de autorización judicial para avanzar sobre información de teléfonos y los problemas de un patrón obtenido sin resguardos. Cautela: la Cámara rechazó la queja fiscal por taxatividad recursiva.

Mora, FBB 3139/2022/1/CA1, Cámara Federal de Bahía Blanca. Ejemplo de línea que admite desbloqueo biométrico compulsivo bajo mínima fuerza y control. Debe citarse como criterio discutido, no como regla nacional.

U., A. C. y otros, justicia penal CABA, 2025. Muestra el debate reciente sobre reconocimiento facial, iris o huella, con voto disidente que ubica la medida en la incoercibilidad. Cautela: sin regla uniforme.

Villalba Cuyari, CABA, Sala I, Causa 11412 (2021). Exige delimitación de la pericia sobre celular, en especial temporal. Útil contra búsquedas de tipo pesca probatoria digital.

CNACC, Sala IV, A., J. A. y otros s/ nulidad, CCC 81978/2018/11/CA9 (2019). Criterio según el cual copiar datos de un teléfono incautado no constituye, por sí, una pericia. Se usa con cautela porque no clausura el problema constitucional del acceso.

13. Errores frecuentes

Afirmación incorrecta	Corrección doctrinaria
Secuestrado el celular, se puede revisar todo su contenido.	Secuestro y acceso son actos distintos; el ingreso al contenido requiere cobertura propia y alcance delimitado.
Si el imputado no desbloquea, eso lo perjudica.	La negativa a aportar PIN o patrón no debe transformarse en indicio de culpabilidad.
La huella o el rostro pueden usarse siempre para abrir el teléfono.	El desbloqueo biométrico compulsivo está discutido y exige análisis de proporcionalidad, coerción y jurisdicción.
Una orden de secuestro habilita a buscar cualquier cosa, por cualquier período.	La orden debe delimitar qué se busca, en qué período y con qué relación con el hecho.
Cualquier defecto anula toda la causa.	Debe distinguirse ilicitud, exclusión, nulidad con perjuicio y peso probatorio.
La pericia técnica sanea cualquier problema previo.	Una pericia correcta no sanea por sí sola un acceso ilícito o desproporcionado.

Conclusión

El contenido de un teléfono puede tener un peso enorme en una causa penal. Ese peso, sin embargo, no surge de haber incautado el aparato, sino de la calidad jurídica y técnica del acceso que permitió leerlo: orden fundada, finalidad concreta, alcance delimitado, preservación, trazabilidad y control. Tener el teléfono no es leer el teléfono.

El problema del desbloqueo confirma la necesidad de matizar. Lo que la persona sabe -su PIN, patrón o contraseña- se ubica en el centro de la garantía contra la autoincriminación. Lo que la persona es -huella, rostro, iris- se mueve en un terreno más discutido, donde algunos tribunales admiten la medida bajo proporcionalidad y otros advierten una lesión a la incoercibilidad.

La conclusión práctica es de método, no de consigna. Distinguir actos, exigir cobertura para el acceso, delimitar la búsqueda y separar las consecuencias de cada defecto. Sin esa disciplina, la prueba digital se vuelve frágil o ilegítima; con ella, la investigación gana solidez y la defensa conserva un terreno real para controlar.

Fuentes y referencias

- Constitución de la Nación Argentina, arts. 18 y 19.
- Código Procesal Penal Federal, arts. 150, 151, 152, 156 y 157.
- Código Procesal Penal de la Nación, art. 253 y reglas de allanamiento, registro, secuestro, custodia y conservación.
- Código Procesal Penal de la Provincia de Buenos Aires, Ley 11.922.
- Ley 26.388 y Ley 27.411, Convenio sobre Ciberdelito.
- Resolución 232/2023 del Ministerio de Seguridad, Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital.
- CSJN, Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986, Fallos 332:111, 24/02/2009.
- CSJN, Quaranta, José Carlos s/ inf. ley 23.737, Fallos 333:1674, 31/08/2010.
- CFCP, Sala I, C., R. E. s/ impugnación, FSA 21955/2019/8/1, Reg. 27/20, 06/10/2020.
- Ríos, FSA 6443/2023/2, Juzgado Federal de Garantías de Tartagal y Cámara Federal de Salta, 2023.
- Mora, FBB 3139/2022/1/CA1, Cámara Federal de Bahía Blanca, 27/05/2022.
- Villalba Cuyari, Cámara de Apelaciones en lo Penal, Penal Juvenil, Contravencional y de Faltas de CABA, Sala I, Causa 11412, 12/10/2021.

- A., J. A. y otros s/ nulidad, CNACC, Sala IV, CCC 81978/2018/11/CA9, 20/09/2019.
- NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics; NIST IR 8387, Digital Evidence Preservation.

Cita sugerida. Selser, Jacobo Iván, *Secuestro del celular y acceso al contenido en el proceso penal argentino: alcance de la orden, código de desbloqueo, biometría y autoincriminación*, ST Abogados, sección Artículos, Buenos Aires, 2026.

Preguntas frecuentes

¿Pueden revisar el contenido de mi celular sin orden judicial?

Secuestrar el teléfono y acceder a su contenido son actos distintos. El ingreso a comunicaciones y datos exige una habilitación propia, fundada y delimitada. Puede haber escenarios de urgencia, pero deben explicarse y documentarse.

¿Me pueden obligar a dar el PIN o el patrón de desbloqueo?

Aportar el PIN o el patrón es un acto cognitivo y voluntario. La línea más sólida lo ubica dentro de la garantía contra la autoincriminación: no debería compelirse ni valorarse en contra la negativa.

¿Y la huella o el reconocimiento facial?

Es un punto discutido. Una línea lo admite como prestación corporal bajo proporcionalidad; otra lo considera alcanzado por la incoercibilidad. No hay una regla nacional uniforme.

¿Qué diferencia hay entre secuestrar y acceder?

El secuestro recae sobre el objeto; el acceso, sobre datos y comunicaciones. El primero exige reglas de incautación y custodia; el segundo exige cobertura específica, finalidad concreta y alcance acotado.

¿Una orden puede autorizar a revisar todo el teléfono?

Una autorización sin recorte temporal ni objetivo se acerca a una exploración general y es más vulnerable. La buena práctica es delimitar qué se busca, en qué período y con qué relación con el hecho.

¿Qué conviene revisar en el acta de secuestro?

Identificación del aparato, IMEI, SIM, estado de bloqueo, hora, lugar, funcionarios, testigos, embalaje, cadena de custodia y si hubo apertura o navegación antes de la pericia.

Anexo A - Matriz de control del acceso a dispositivos

Eje	Pregunta que responde	Qué permite sostener	Límite
Licitud del acceso	¿Había cobertura para ingresar al contenido?	Validez constitucional y procesal del ingreso.	Una pericia correcta no sanea un acceso ilícito.
Alcance	¿Hasta dónde se autorizó buscar?	Delimitación temporal y objetiva de la medida.	La orden genérica se acerca a una exploración general.
Clave	¿Se exigió el PIN o patrón?	Respeto de la garantía contra la autoincriminación.	La negativa no debe valorarse en contra.
Biometría	¿Hubo desbloqueo biométrico compulsivo?	Discusión de incoercibilidad y proporcionalidad.	Materia controvertida, sin regla uniforme.
Cadena de custodia	¿Quién tomó contacto con el aparato y el archivo?	Identidad, estado y conservación.	Requiere demostrar tramo físico y digital.
Terceros	¿Se afectó a personas ajenas al proceso?	Proporcionalidad de la injerencia.	El exceso debilita la medida y la prueba.

Anexo B - Checklist defensivo

- Orden: si autorizaba sólo el secuestro del objeto o también el acceso a datos, copia, búsqueda y pericia.
- Acta de secuestro: hora, lugar, funcionarios, testigos, marca, modelo, IMEI, SIM, estado de bloqueo y embalaje.
- Acceso: si hubo apertura, encendido, navegación o captura previa a la pericia, y con qué cobertura.

- Clave: si se exigió el PIN o patrón, o si se valoró en contra la negativa a aportarlo.
- Biometría: si hubo desbloqueo compulsivo, qué orden lo fundó y qué proporcionalidad se explicó.
- Cadena de custodia: del dispositivo y del archivo, con identificación de quienes tomaron contacto.
- Método y herramienta: tipo de extracción, software, versión, operador, hash y límites de búsqueda.
- Control: notificación a la defensa, posibilidad de consultor técnico y acceso al informe completo.
- Alcance: si la búsqueda fue temporal y objetivamente acotada o una exploración general.
- Consecuencia: distinguir ilicitud y exclusión, nulidad con perjuicio, o mera discusión de peso probatorio.

Anexo C - Checklist para querella o acusación

- Asegurar y aislar el dispositivo para evitar borrado remoto o sincronización, sin explorar su contenido.
- Solicitar una orden que cubra expresamente el acceso a datos, y no sólo el secuestro del objeto.
- Delimitar la búsqueda por franja temporal, aplicaciones, tipos de datos o palabras clave vinculadas al hecho.
- Obtener el acceso por vías técnicas, sin trasladar al imputado el deber de aportar la clave.
- Documentar la voluntariedad cuando el material es entregado por víctima o testigo.
- Pedir extracción forense cuando se discutirán autenticidad, integridad, autoría o contexto.
- Preservar cadena de custodia del aparato y del archivo, con trazabilidad y valores de integridad cuando corresponda.
- Resguardar la intimidad de terceros y separar lo relevante de lo ajeno al proceso.
- Explicar al tribunal cómo cada paso técnico se relaciona con el hecho imputado.

Nota editorial

Este trabajo tiene finalidad informativa y doctrinaria. No constituye asesoramiento legal para un caso concreto. La validez y eficacia de la evidencia digital dependen de la jurisdicción, la etapa procesal, la forma de obtención, la cadena de custodia, la posibilidad de control técnico y el resto del cuadro probatorio.