

Santiago, veintinueve de septiembre de dos mil veintiséis.

Vistos y teniendo presente:

Primero: Que comparece Hugo Humberto Gutiérrez Gálvez, abogado, por sí y en su propio favor, e interpone acción constitucional de amparo en contra de Daniela Verónica Guerrero González, jueza del Cuarto Juzgado de Garantía de Santiago, por la resolución que dictó el 26 de agosto de 2026 en la audiencia de cautela de garantías celebrada en la causa RUC 2600858361-6, RIT O-6719-2026, en cuanto permitió al Ministerio Público y a las policías acceder al contenido del teléfono celular que le fue incautado y examinarlo, sin fijar un mecanismo de control judicial previo que excluya del conocimiento del persecutor las comunicaciones amparadas por el secreto profesional y las mantenidas con terceros ajenos a los hechos investigados.

Estima que esa decisión es ilegal, porque autoriza la injerencia del persecutor en comunicaciones privadas protegidas sin sujeción a los resguardos que el ordenamiento contempla, y arbitraria, porque el tribunal reconoció que la Fiscalía tendrá acceso a información impertinente y privada sin ponderar alternativas menos lesivas, como el protocolo de revisión segmentada que su defensa propuso en la audiencia. Sostiene que con ello se amenaza su seguridad individual y su libertad personal, garantizadas en el artículo 19 N° 7 letra b) de la Constitución Política de la República, en relación con el respeto a la vida privada y la inviolabilidad de las comunicaciones privadas que aseguran los numerales 4° y 5° del mismo artículo.

En cuanto a los hechos, expone que en una investigación por delitos de cohecho, soborno y lavado de activos, entre otros, el 20 de agosto de 2026 entregó voluntariamente su teléfono en la Brigada Anticorrupción de la Policía de Investigaciones, requerido en virtud de una resolución de incautación que no le fue exhibida por estar reservada la causa y a la que no ha tenido acceso. Ese mismo día pidió audiencia de cautela de garantías conforme al artículo 10 del Código Procesal Penal, a fin de obtener el control judicial de la incautación y medidas de resguardo respecto del acceso, revisión y extracción del contenido del aparato. En la audiencia, celebrada el 26 de agosto de 2026, su defensa supo que la investigación se encuentra reservada con arreglo al artículo 31 de la Ley N° 19.913 por seis



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: FMYDXKZUUP

meses contados desde el 24 de julio de 2026, y solicitó que se regulara judicialmente el acceso del Ministerio Público al celular, para resguardar las comunicaciones con clientes y con otras personas ajenas a los hechos.

Indica que el tribunal acogió parcialmente la petición, pues circunscribió la búsqueda de información al período comprendido entre el año 2018 y el 20 de agosto de 2026 y prohibió incorporar a la carpeta investigativa la información ajena a los hechos, pero rechazó expresamente todo mecanismo de control o filtro previo, sosteniendo que “no es posible una exclusión ex ante de parte de la información contenida en los dispositivos”, que las defensas tendrán, de existir una vulneración, la posibilidad de solicitar la exclusión del medio probatorio, y que “no cabe duda que el persecutor tendrá acceso a información que será ciertamente impertinente y privada”. De este modo, agrega, la resolución posterga la protección de las garantías a un control *ex post*, meramente eventual, que no repara la afectación consumada.

En cuanto al derecho, sostiene que el secreto profesional del abogado, que tiene naturaleza de derecho y de deber, está reconocido en los artículos 8.1 y 8.2 letra d) de la Convención Americana sobre Derechos Humanos y 14.3 letra b) del Pacto Internacional de Derechos Civiles y Políticos, en los Principios básicos sobre la función de los abogados aprobados por las Naciones Unidas en 1990 y en la sentencia de la Corte Interamericana de Derechos Humanos en el caso Tristán Donoso vs. Panamá; que los artículos 220 y 303 del Código Procesal Penal proyectan esa protección a las comunicaciones con clientes ajenos a la causa, la que perdería toda eficacia frente a una extracción masiva; y que el dispositivo contiene información de más de 35 años de defensa de los derechos humanos, resguardada además por el secreto de 50 años que el artículo 15 de la Ley N° 19.992 establece respecto de los antecedentes aportados ante la Comisión Nacional sobre Prisión Política y Tortura. Añade que, al rechazar todo filtro previo, el tribunal dejó en manos del persecutor, parte interesada, la determinación de lo pertinente, en contra del control judicial previo que exige el artículo 9° del mismo Código, y que la resolución omitió toda referencia al secreto profesional, con infracción de su artículo 36.

Pide que se acoja el amparo, se declare la ilegalidad y arbitrariedad de la resolución en cuanto decreta el acceso al teléfono sin control judicial



previo y específico, y se ordene la prohibición absoluta de acceso a toda comunicación amparada por el secreto profesional y las garantías de privacidad, intimidad e inviolabilidad de las comunicaciones, así como la designación de un ministro de fe de esta Corte o de un juez de garantía distinto que supervise un protocolo estricto de exclusión, con segregación de la información antes de que la Fiscalía o la policía la examinen. Ese protocolo debería fijar, según el recurso, los hechos investigados, un período determinado, las personas, números y cuentas respecto de los cuales pueda buscarse, las categorías de información autorizadas, la exclusión de lo relativo a patrocinados, abogados y otras causas, un registro técnico de los parámetros de búsqueda y el resguardo del aparato en la Fiscalía.

Segundo: Que Daniela Verónica Guerrero González, jueza titular del Cuarto Juzgado de Garantía de Santiago, evacuó el informe que le fue requerido y solicitó tener presente que, salvo mejor parecer de esta Corte, la resolución impugnada no vulnera derecho constitucional alguno y fue dictada con estricta sujeción a la ley.

Expone que en la audiencia de 26 de agosto de 2026, celebrada para controlar las garantías de los imputados conforme al artículo 10 del Código Procesal Penal, las defensas de cuatro investigados, entre ellas la del amparado, pidieron copia de la solicitud que motivó la resolución de 18 de agosto de 2026 y que se regulara judicialmente el acceso del Ministerio Público y de las policías a los dispositivos electrónicos incautados, a lo que el persecutor se opuso. El tribunal rechazó la entrega de copias, por tratarse de antecedentes de la investigación sujetos a la reserva decretada por el Ministerio Público el 24 de julio de 2026 con arreglo al artículo 31 de la Ley N° 19.913, y razonó que toda medida intrusiva afecta derechos y garantías, motivo por el cual exige autorización judicial previa, la que en este caso se dictó el 18 de agosto de 2026, y que la naturaleza de los delitos de corrupción explica que tales autorizaciones se otorguen sin conocimiento del afectado y en una investigación reservada.

Descartó luego la aplicación del artículo 220 del Código Procesal Penal al abogado que tiene la calidad de imputado, sin perjuicio de precisar que no es parte de la investigación indagar en las comunicaciones que en esa calidad mantenga con sus clientes, las que estarán a resguardo en la



medida en que no se relacionen con los hechos investigados. Estimó que no es posible una exclusión *ex ante* de parte de la información, que la entrega de ésta no puede quedar al arbitrio de la persona investigada y que limitar el examen conforme a criterios previos importaría una intromisión indebida en las facultades del persecutor y entorpecería el análisis, quedando a salvo la posibilidad de solicitar en su oportunidad la exclusión del medio probatorio. Reconoció, con todo, que el persecutor tendrá acceso a información impertinente y privada y que no es posible limitar esa posibilidad sin riesgo de frustrar la investigación.

En consecuencia, acogió la segunda solicitud sólo en cuanto la búsqueda de la información relativa a los hechos investigados deberá circunscribirse al período comprendido entre el año 2018 y el 20 de agosto de 2026, fecha de la incautación; prohibió la entrega a los intervinientes o a terceros, y la incorporación a la carpeta investigativa, de toda información contenida en los dispositivos ajena a los hechos; y ordenó al Ministerio Público sujetar su actuación a los instructivos contenidos en sus oficios 363/2025 y 983/2024, respecto de los cuales advirtió que dejan a salvo varias de las aprehensiones de los litigantes y que el tribunal no tenía inconveniente en que se plantearan complementaciones destinadas a limitar o aclarar el alcance de lo resuelto.

En cuanto al derecho, afirma que la resolución se ajusta a la normativa aplicable a los delitos económicos y a lo dispuesto en el artículo 220 del Código Procesal Penal, precepto que no rige respecto de quienes, como el recurrente, son imputados en la investigación cuyo objeto se pretende sustraer del conocimiento del persecutor. Señala que no es controvertido que la investigación no guarda relación con el ejercicio profesional del recurrente en materia de derechos humanos, lo que descarta el riesgo de comprometer información amparada por el secreto profesional vinculada a esas causas; que el tribunal ya ponderó esa eventualidad al circunscribir la búsqueda y prohibir la entrega e incorporación de lo ajeno a los hechos; que, si en el examen se detecta información protegida, el amparado conserva íntegro su derecho a solicitar la exclusión del medio de prueba; y que la forma en que el Ministerio Público organiza internamente la revisión del material incautado pertenece a la esfera de autonomía que el artículo 83 de la Constitución Política le reconoce en la dirección exclusiva



de la investigación, sin que corresponda al tribunal prescribir la metodología de esa revisión.

Tercero: Que el Ministerio Público, por intermedio de la fiscal adjunta de la Fiscalía de Alta Complejidad y Crimen Organizado de la Fiscalía Regional Metropolitana Oriente a cargo de la investigación, acompañó, con ocasión de la vista de la causa, el Oficio FN N° 983/2024, de 16 de octubre de 2024, que imparte criterios de actuación en investigaciones penales complejas para el otorgamiento de copias, solicitud de diligencias y registro de información personal de interés investigativo, y el Oficio FN N° 363/2025, de 4 de abril de 2025, que lo complementa, a los que remite la resolución impugnada. De su contenido se dará cuenta más adelante. En estrados, el Ministerio Público no informó el estado en que se encuentra la extracción del contenido del teléfono, si ella se completó o está pendiente, si se elabora un informe con su resultado ni la forma en que se conduce o conducirá la búsqueda de la información pertinente.

Cuarto: Que la acción constitucional de amparo, consagrada en el artículo 21 de la Constitución Política de la República, constituye un mecanismo de tutela de urgencia cuyo propósito es que la magistratura adopte de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado, frente a toda privación, perturbación o amenaza a su derecho a la libertad personal y seguridad individual que provenga de un acto u omisión contrarios a la Carta Fundamental o a las leyes.

Quinto: Que, como se advierte, el recurrente impugna la resolución que el Cuarto Juzgado de Garantía de Santiago dictó el 26 de agosto de 2026 en la causa RIT O-6719-2026, en cuanto permite al Ministerio Público y a las policías acceder al contenido íntegro de su teléfono celular sin un mecanismo de control o filtro previo, lo que, a su juicio, amenaza su seguridad individual en relación con la vida privada y la inviolabilidad de las comunicaciones. La recurrida no niega el hecho, sino que justifica su decisión en la ley y en los resguardos que adoptó, que estima suficientes. La cuestión a resolver consiste, entonces, en determinar si la jueza de garantía, al pronunciarse sobre la cautela pedida, satisfizo los deberes que la Constitución y el Código Procesal Penal le imponen respecto de una diligencia que ella misma reconoció como lesiva de la privacidad del



amparado y de terceros, o si, por el contrario, dejó la ejecución de esa diligencia sin el control que aquéllos exigen.

Sexto: Que, antes de entrar al fondo, conviene dejar sentado que la procedencia de esta acción ya fue resuelta. La Primera Sala de esta Corte la declaró inadmisibile el 3 de septiembre de 2026, por estimar que los hechos invocados se vinculan con la privacidad, la inviolabilidad de las comunicaciones y el secreto profesional y no con las hipótesis que resguarda el artículo 21 de la Constitución; apelada esa resolución, la Corte Suprema la revocó el 17 de septiembre de 2026, en los autos Rol N° 49.688-2026, por considerar que la situación descrita en el recurso sí puede constituir uno de los supuestos previstos en ese precepto, y dispuso que una sala no inhabilitada diera al amparo la tramitación correspondiente “a fin de pronunciarse derechamente sobre el amparo deducido”.

Esa decisión se aviene con la doctrina que el máximo tribunal ha sostenido en casos semejantes, según la cual la libertad personal y la seguridad individual pueden verse amenazadas no sólo por vía principal, sino también de modo consecuencial, esto es, “con ocasión de la ejecución de un acto lesivo de uno o más derechos distintos”, y en ambos supuestos el amparo es el mecanismo idóneo para dejar sin efecto lo que ilegítimamente ponga en riesgo su ejercicio, pues reducir la acción a las afectaciones directas “importaría una injustificada restricción al derecho de accionar en procura de acceder a una tutela judicial efectiva” (SCS rol 12.292-2025, 28 de abril de 2025; en el mismo sentido, SCS rol 16.420-2025, 22 de mayo de 2025).

Por consiguiente, no corresponde a esta Sala volver sobre la admisibilidad y debe pronunciarse derechamente sobre la infracción denunciada.

Séptimo: Que los hechos relevantes no están discutidos. El 19 de agosto de 2026, en la investigación reservada que se sigue por delitos previstos en la Ley N° 20.393, fraude al fisco, fraude informático, delitos contra la salud pública, falsificación de instrumento privado, cohecho y lavado de activos, la jueza Francis Fell Franco, del mismo Cuarto Juzgado de Garantía de Santiago, autorizó por diez días la entrada y registro de diversos domicilios y la incautación de teléfonos celulares, computadores y demás dispositivos de almacenamiento digital de titularidad de las personas



que individualizó, entre ellas el amparado, “que pudieran dar cuenta de reuniones, intercambios de información y otras formas de comunicación relacionadas a los hechos investigados”, y autorizó al persecutor y a la policía “el acceso, revisión, extracción y análisis de la información contenida en los dispositivos electrónicos incautados”, comprensiva de sus memorias internas y externas, de la tarjeta SIM, de las imágenes, videos, audios y de todo dato y registro almacenado en ellos, “así como en sus aplicaciones, redes sociales, correos electrónicos y nubes de almacenamiento a las que se halle vinculado el dispositivo”, sin acotar el período ni las materias de interés. Es la resolución a la que el informe y la resolución recurrida se refieren como de 18 de agosto. El 20 de agosto el amparado entregó su teléfono a la Policía de Investigaciones y pidió la cautela de sus garantías; y el 26 de agosto la jueza recurrida, al resolverla, acotó temporalmente la búsqueda, prohibió entregar e incorporar a la carpeta lo ajeno a los hechos y remitió a dos instructivos internos del Ministerio Público, pero declinó fijar cualquier otro límite a la ejecución de la extracción, con la advertencia de que el persecutor accederá a información impertinente y privada. Lo que se examina, por ende, no es la legalidad de la incautación ni la de la autorización para revisar el aparato, que el recurrente no impugna, sino la suficiencia de los términos en que el tribunal dejó que esa revisión se ejecute.

Octavo: Que la respuesta exige partir de lo que hoy es un teléfono inteligente. Ningún otro objeto concentra tanta información sobre una persona. Acompaña a su dueño a toda hora; por él transitan sus conversaciones, sus fotografías, sus pagos y sus cuentas bancarias, su trabajo y la administración de su casa, y en su memoria se superponen, sin separación posible, la vida laboral, la doméstica y la afectiva. Tampoco admite, a diferencia del domicilio, un acotamiento espacial, pues en una casa puede registrarse una habitación y dejar cerradas las demás, mientras que quien accede a un teléfono accede a todo lo que contiene. La Corte Suprema de los Estados Unidos lo describió en *Riley v. California*. Estos aparatos, dijo, son en realidad minicomputadores que reúnen en un solo lugar distintas clases de información, cuya combinación revela mucho más que cualquiera de ellas por separado; la suma de la vida privada de una persona puede reconstruirse a partir de un millar de fotografías fechadas y



localizadas; la mayoría de sus dueños lleva consigo “un registro digital de casi todos los aspectos de sus vidas”; y un registro del teléfono “expondría típicamente al gobierno mucho más que el registro más exhaustivo de una casa” (Riley v. California, 573 U.S. 373, 393-397 y 403, 2014).

La misma idea llevó al Tribunal Constitucional Federal alemán a reconocer un derecho fundamental autónomo a la confidencialidad e integridad de los sistemas informáticos, comprensivo de los teléfonos móviles con múltiples funciones, al constatar que el acceso estatal a sistemas que contienen datos personales en tal cantidad y variedad permite reconstruir aspectos esenciales de la vida de una persona e incluso elaborar un perfil completo de su personalidad, y que ese riesgo existe ya en medidas de acceso aislado, como la incautación o copia de los soportes de almacenamiento, cuyos registros pueden incluir la correspondencia privada y profesional y anotaciones de carácter íntimo (BVerfG, sentencia de 27 de febrero de 2008, 1 BvR 370/07 y 1 BvR 595/07, BVerfGE 120, 274). El mismo tribunal advirtió que la gravedad de la injerencia aumenta cuando los datos revelan las comunicaciones del afectado con terceros, ya que la medida alcanza indiscriminadamente a esos interlocutores, respecto de los cuales no concurren los presupuestos que la justifican (ibídem).

Lo dicho vale, con igual o mayor razón, para los computadores y demás dispositivos de almacenamiento masivo de información, que contienen datos de la misma naturaleza y se examinan del mismo modo, de manera que los razonamientos de esta sentencia les son aplicables con las adaptaciones que su distinta configuración exija. Si el análisis se centra en el teléfono es porque en él concurren con mayor intensidad las características descritas y porque es el único aparato cuya incautación al amparado consta en estos antecedentes, aunque la resolución de 19 de agosto de 2026 autorizó también la de computadores, discos duros y otros soportes.

Noveno: Que a esa constatación se suma la forma en que la diligencia se ejecuta. La revisión de un teléfono incautado no consiste en abrir una carpeta determinada, sino en obtener, mediante herramientas forenses, una copia íntegra de su contenido, la llamada copia espejo, sobre la cual se practica después la búsqueda de lo pertinente. Al extraer, la técnica no distingue lo útil de lo que no lo es; se copia todo, desde los



registros de las aplicaciones de mensajería y de correo hasta las fotografías, incluida la información personal, íntima y familiar del titular, y sólo con posterioridad se determina qué sirve a la investigación. Desde el punto de vista jurídico, generar esa copia equivale a apoderarse de todos los datos aunque el aparato se devuelva, porque el funcionario que la obtiene no sabe qué contenido ha copiado, sino sólo que ha tomado una copia de cuanto había en el dispositivo (Kerr, O. S., “Fourth Amendment Seizures of Computer Data”, en Yale Law Journal, vol. 119, 2010, pp. 709 y 717).

Por eso la lesión no se atenúa por la circunstancia de que el persecutor, una vez en posesión del acervo completo, seleccione después lo que quiere examinar, que es el supuesto del que parte la resolución recurrida cuando remite la protección a la exclusión probatoria posterior. La injerencia se consuma con la copia, no con el uso; desde ese momento el Estado dispone de toda la información y el afectado depende de la buena disposición del órgano que la tiene. La Corte Suprema estadounidense lo advirtió recientemente a propósito de los registros de localización que un servicio conserva de sus usuarios, al sostener que el alcance de la invasión “no se hace menor porque el gobierno, con el beneficio de la retrospectiva, pueda señalar exactamente qué pocas horas de desplazamientos quiere revisar” (Chatrie v. United States, No. 25-112, sentencia de 29 de junio de 2026, slip op. p. 21). En términos análogos, el Tribunal Europeo de Derechos Humanos ha subrayado que la separación de lo protegido y lo que no lo está adquiere especial relevancia cuando la incautación recae sobre grandes volúmenes de datos digitales o se practica mediante una copia espejo, y que resulta esencial impedir todo acceso no autorizado ni registrado a esos datos desde su incautación hasta su devolución o destrucción (TEDH, Särgava c. Estonia, N° 698/19, 16 de noviembre de 2021). De ahí que el control no pueda diferirse al momento en que el persecutor decida usar la información, sino que deba recaer sobre la conservación misma de la copia, que es donde reside la afectación.

En el caso, la resolución recurrida da cuenta de esa realidad. La jueza dejó constancia de que “no es posible una exclusión ex ante de parte de la información contenida en los dispositivos” y de que “no cabe duda de que el persecutor tendrá acceso a información que será impertinente y privada”. La



afectación que aquí se examina no es, entonces, hipotética ni discutida; está reconocida en el acto impugnado y se extiende a terceros que no son imputados, como los familiares cuyas fotografías y mensajes alberga el aparato o las personas que se comunicaron con el amparado, cuya privacidad quedará expuesta sin que a su respecto concorra sospecha alguna.

A ello se agregan dos circunstancias propias de este caso. La primera es la condición de abogado del amparado, con una trayectoria de más de 35 años en la defensa de los derechos humanos, según expone. Su teléfono no contiene sólo información suya; contiene la que sus clientes le confiaron en asuntos ajenos a esta investigación, cubierta por el deber de secreto que el artículo 303 del Código Procesal Penal reconoce y que pertenece a esos terceros y no al abogado, y, según afirma, antecedentes aportados por víctimas ante la Comisión Nacional sobre Prisión Política y Tortura, cuyo secreto legal por cincuenta años invoca con arreglo al artículo 15 de la Ley N° 19.992. La jueza recurrida reconoció que indagar en esas comunicaciones no es parte de la investigación. Se trata, pues, de información que ni el persecutor ni terceros debieran llegar a conocer, y que por lo mismo debe quedar excluida de la búsqueda y eliminada de la copia obtenida o que se esté obteniendo, como se dispondrá. El Tribunal Europeo de Derechos Humanos ha exigido garantías procedimentales específicas cuando el material incautado o copiado es el de un abogado, incluso cuando es él mismo el sospechoso, porque lo protegido es la confianza de sus clientes y la posición que la abogacía ocupa en la administración de justicia, y ha reprochado que la orden de registro se limite a señalar que los investigadores accederán sólo a los datos relevantes, sin prever resguardo concreto alguno para el material amparado por el secreto (*Särgava c. Estonia*; *Nezirić c. Bosnia y Herzegovina*).

La segunda es que, hasta ahora, ninguna otra limitación se ha fijado. Como se dejó constancia, en estrados el Ministerio Público no informó el estado de la extracción, si ésta se completó o está pendiente, si se elabora un informe con su resultado ni cómo se conduce la búsqueda dentro de la copia; y la resolución de 19 de agosto de 2026 autorizó el acceso a todo el contenido del aparato y de los servicios vinculados a él sin acotar materias, personas ni período. El único patrón que hoy delimita el examen es el



temporal que la jueza recurrida impuso el 26 de agosto. Todo lo demás, esto es, qué se busca, con qué criterios, quiénes acceden y qué ocurre con lo que no interesa, queda librado al arbitrio del órgano que ejecuta la diligencia.

Décimo: Que la intromisión no se agota en la memoria del aparato. El teléfono es, además, la llave de acceso a los servicios que su titular mantiene con la sesión abierta, esto es, cuentas de correo, redes sociales de acceso restringido, mensajería sincronizada y repositorios de almacenamiento en la nube, cuyos contenidos no residen en el dispositivo sino en servidores remotos, con frecuencia situados fuera del país, y a los que se llega con sólo pulsar la pantalla. Quien examina un teléfono desbloqueado puede alcanzar por esa vía información que nunca estuvo en poder de la policía, que el titular considera suya aunque la custodie un tercero y que en muchos casos pertenece también a otras personas, como ocurre con los grupos de mensajería, los perfiles cerrados de una red social o las carpetas compartidas. La Corte Suprema de los Estados Unidos advirtió en *Riley* que los datos que el usuario ve en su teléfono pueden no estar almacenados en él, que los agentes que revisan el aparato no sabrán normalmente si lo que miran estaba en el dispositivo o proviene de la nube, y que extender a esos archivos el registro del teléfono sería como encontrar una llave en el bolsillo de un sospechoso y sostener que ella autoriza a abrir y registrar una casa (*Riley v. California*, 573 U.S. 373, 397-398); y en *Chatrre* agregó que los registros que un servicio guarda en sus servidores se asemejan a los correos, documentos, fotografías o calendarios que el usuario razonablemente considera propios aunque estén alojados en servidores ajenos (*Chatrre v. United States*, slip op. p. 18). El Tribunal Constitucional Federal alemán, por su parte, incluyó expresamente en el ámbito del derecho a la confidencialidad e integridad de los sistemas informáticos los datos a los que el sistema da acceso en virtud de sus conexiones de red (BVerfG, sentencia de 27 de febrero de 2008).

Entre nosotros ese salto no es de cantidad sino de naturaleza. El acceso remoto a un dispositivo, computador o sistema informático mediante programas computacionales, contraseñas, códigos de seguridad o de acceso es una diligencia distinta, que el artículo 225 bis del Código Procesal Penal somete a petición fundada del Ministerio Público, a la existencia de



fundadas sospechas basadas en hechos determinados y a una autorización judicial específica, sujeta a un plazo máximo y a los requisitos de contenido que detalla el artículo 225 ter. Servirse de la sesión abierta en el teléfono incautado para ingresar a esos repositorios produce el mismo efecto que el registro remoto, con la diferencia de que se obtiene sin la resolución fundada que la ley exige para él; por eso no puede entenderse comprendido en la autorización para revisar el contenido del aparato y requiere una autorización expresa, que precise el servicio, la cuenta y el alcance del acceso. La Ley de Enjuiciamiento Criminal española lo resuelve en esos términos, al exigir autorización judicial para ampliar el registro desde el dispositivo incautado a los datos almacenados en otro sistema informático accesible desde él, salvo que la autorización inicial ya la comprenda, según su artículo 588 sexies c, apartado 3. En este caso, la resolución de 19 de agosto de 2026 extendió la autorización, en términos genéricos, a las aplicaciones, redes sociales, correos electrónicos y nubes de almacenamiento a las que se halle vinculado el dispositivo, sin individualizar servicios ni cuentas, sin acotar el período y sin las especificaciones que el artículo 225 ter exige para el registro remoto. Esa autorización no ha sido impugnada por esta vía, pero su ejecución queda comprendida en el problema que aquí se resuelve, pues el acceso a esos repositorios multiplica el volumen de información privada, del amparado y de terceros, que el persecutor obtendrá. De ahí que las medidas de control que se dispondrán deban alcanzarlo, y que el Ministerio Público deba informar al tribunal a qué servicios y cuentas ha accedido o accederá por esa vía, para que el juez de garantía delimite ese acceso con arreglo a los artículos 225 bis y 225 ter.

Undécimo: Que la lesión así descrita no proviene de la ley, que nada dice sobre la revisión del teléfono incautado, sino de la resolución judicial que autoriza la diligencia y fija, o deja de fijar, sus términos. El artículo 9° del Código Procesal Penal somete a autorización judicial previa toda actuación del procedimiento que prive al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o los restrinja o perturbe, y el inciso segundo del artículo 5° ordena interpretar restrictivamente las disposiciones que autorizan la restricción de la libertad o de otros derechos del imputado. Si la ley confía al juez esa autorización, es porque espera de él algo más



que un permiso; espera que pondere la intensidad de la injerencia frente al interés de la persecución y que la limite a lo que ese interés requiere. El principio de proporcionalidad, con sus exigencias de idoneidad, necesidad y proporcionalidad en sentido estricto, es el método con que esa ponderación se realiza, y la doctrina nacional ha sostenido que el juez de garantía debe practicar ese test antes de decretar cualquier medida restrictiva de derechos fundamentales, comprobando que la diligencia sea adecuada al fin que se pretende, eligiendo entre las medidas idóneas la menos lesiva y verificando que las ventajas de la autorización guarden correspondencia con la vulneración que causa (Núñez Ojeda, R., Beltrán Calfurrapa, R. y Santander Akkrass, N., “Los hallazgos casuales en las diligencias de incautación e intervención de las comunicaciones digitales en Chile. Algunos problemas”, en *Política Criminal*, vol. 14, N° 28, 2019, pp. 159-160 y 180).

La Corte Suprema ha situado esa exigencia en el centro del control de las diligencias intrusivas, al declarar que el tribunal está obligado a requerir del persecutor las precisiones necesarias para despejar cualquier situación incierta, “principalmente para satisfacer correctamente el estándar de proporcionalidad que conlleva acceder a una diligencia invasiva de derechos fundamentales” (SCS rol 12.292-2025, 28 de abril de 2025). Trasladado ese estándar a la revisión de un teléfono, el juicio de necesidad impone al juez adoptar las medidas que reduzcan la afectación de la privacidad al mínimo compatible con el éxito de la investigación, y ello con mayor razón cuando la injerencia alcanza a terceros ajenos al proceso, que no han sido oídos ni pueden defenderse. Una autorización que reconoce que el persecutor accederá a información impertinente y privada y, en el mismo acto, renuncia a fijar cómo se acotará ese acceso y qué ocurrirá con lo excedente, no supera ese juicio.

Duodécimo: Que la intensidad de esta injerencia es, cuando menos, equivalente a la de las medidas que el Código sí regula con detalle. La interceptación de comunicaciones capta lo que se dice mientras se dice; el registro remoto de equipos informáticos aprehende el contenido de un sistema sin conocimiento del usuario; la extracción del teléfono incautado toma de una vez todo lo que se dijo, se escribió, se fotografió y se guardó durante años. Para las dos primeras el legislador exige fundadas sospechas basadas en hechos determinados. Sujeta la interceptación a delitos con



pena de crimen y a que la investigación la haga imprescindible, y ordena que la resolución individualice al afectado, singularice los medios a intervenir y señale al funcionario encargado, la forma, el alcance y la duración de la medida, que no puede exceder de sesenta días prorrogables sólo previo examen de la subsistencia de sus requisitos, como dispone el artículo 222; y limita el registro remoto a un plazo máximo de treinta días, prorrogable bajo la misma condición, conforme al artículo 225 bis. El artículo 225 ter, a su vez, exige que la resolución que autoriza el acceso remoto especifique los dispositivos objeto de la medida, “el alcance de la medida, la forma en la que se procederá al acceso y aprehensión de contenidos relevantes para la causa”, los agentes autorizados, la autorización para realizar y conservar copias, las medidas técnicas de preservación y “la duración precisa de la medida”. Y, cumplida la interceptación, el inciso cuarto del artículo 223 manda entregar a los afectados las comunicaciones impertinentes o irrelevantes y ordena que el Ministerio Público destruya toda transcripción o copia de ellas.

La Corte Suprema ha recordado que, por ser excepcionales las medidas que afectan la intimidad, la vida privada y la inviolabilidad de las comunicaciones, “el legislador exige un alto estándar de exigencias que deben cumplirse tanto por la fiscalía -para solicitarlas- como de motivación por el juez al dictar la resolución que las dispone” (SCS rol 18.430-2025, 3 de junio de 2025). No sería coherente que la diligencia más invasiva de todas, la que abarca a la vez las comunicaciones pasadas, las imágenes, los documentos, los desplazamientos y las relaciones del titular con terceros, quedara sometida a exigencias menores que la interceptación o el registro remoto por el solo hecho de que el Código, promulgado en el año 2000, cuando los teléfonos móviles no tenían las capacidades actuales, no la menciona, silencio que las reformas posteriores no han llenado, ni siquiera la Ley N° 21.577, que reguló el registro remoto de equipos informáticos, a diferencia de lo ocurrido en España, donde desde 2015 la ley disciplina de modo específico el registro de los dispositivos de almacenamiento masivo de información. El principio de proporcionalidad conduce a lo contrario, pues obliga a exigir de la petición del persecutor y de la resolución que la acoge, al menos, el mismo nivel de fundamentación y de precisión que el legislador impone a aquéllas.



Ninguna objeción cabe oponer a que esas exigencias se extiendan por vía analógica a una diligencia que la ley no regula. La prohibición de analogía del inciso segundo del artículo 5° del Código Procesal Penal alcanza a las disposiciones que autorizan la restricción de la libertad o de otros derechos del imputado, no a las que la condicionan o limitan; trasladar a la revisión del teléfono incautado los resguardos previstos para el registro remoto opera en beneficio del afectado y responde al deber que el inciso segundo del artículo 5° de la Constitución impone a los órganos del Estado de respetar y promover los derechos esenciales que emanan de la naturaleza humana. Por lo demás, si el acceso clandestino a un sistema informático debe acotarse en su alcance, forma, agentes, copias y duración, no se advierte por qué habría de quedar exento de esos límites el acceso que, sin ser clandestino, es compulsivo e impuesto, pues en uno y otro caso falta la voluntad del usuario para el registro y revisión de sus datos, y ante un grado equivalente de afectación de la garantía corresponden resguardos equivalentes.

El derecho comparado confirma esta orientación. La Ley de Enjuiciamiento Criminal española somete las medidas de investigación tecnológica a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, declara que “la simple incautación” de un teléfono u otro dispositivo de almacenamiento masivo “no legitima el acceso a su contenido”, exige una motivación individualizada para autorizarlo y dispone que la resolución que lo permite “fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos”, según sus artículos 588 bis a) y 588 sexies a), b) y c). Allí donde el legislador ha regulado la materia, en suma, no ha admitido que el acceso al contenido de un teléfono siga automáticamente a su incautación ni que la orden pueda omitir el alcance del registro y el destino de las copias.

Décimo tercero: Que de lo anterior se sigue el contenido mínimo que debe tener la resolución que autoriza la extracción y revisión de un teléfono. No basta con permitir el “peritaje” o el “vaciado” del aparato, porque sin determinación del objeto no hay modo de saber después qué fue búsqueda y qué fue hallazgo. El artículo 36 del Código Procesal Penal obliga a expresar “sucintamente, pero con precisión, los motivos de hecho y de derecho” de la decisión, y la Corte Suprema ha declarado que ese mandato



integra las garantías mínimas del debido proceso y no se satisface con la mera relación de los antecedentes o de las solicitudes de los intervinientes (SCS rol 14.900-2024, 9 de mayo de 2024; SCS rol 12.292-2025, 28 de abril de 2025). Aplicado a esta diligencia, el deber de fundamentación exige que el juez requiera del Ministerio Público, y consigne en su resolución, cuál es la información que se busca, determinada por los hechos investigados, las personas o cuentas con las que se pretende establecer comunicación, la época a que se refiere y las categorías de contenido pertinentes, así como la manera en que, obtenida la copia íntegra, se identificará lo útil y el plazo dentro del cual lo restante será eliminado de esa copia. Si el persecutor sostiene que alguna de esas determinaciones es técnicamente imposible, a él corresponde justificarlo ante el juez, y no al afectado demostrar lo contrario.

La proposición de esos criterios corresponde al Ministerio Público y no al juez. Definir los descriptores de una búsqueda dirigida, sean palabras clave, interlocutores, cuentas, tipos de archivo o rangos de fechas, es una función investigativa que exige el dominio de los antecedentes reunidos, de la hipótesis que se indaga y de las técnicas forenses e informáticas con que se examina una copia, conocimientos que el tribunal no posee y que el artículo 83 de la Constitución radica en el persecutor. Lo que el juez puede y debe exigir es que esa propuesta exista antes de que la copia se examine, que quede registrada, que sea puesta en su conocimiento y que sea razonable, pues sólo así el control posterior contará con un punto de referencia contra el cual medir lo que se hizo. Este último requisito no es menor. Unos criterios tan amplios que capturen la mayor parte del contenido, como sería buscar por términos de uso corriente o por interlocutores indeterminados, equivalen a no tener criterios, y bajo su apariencia la revisión termina por abarcarlo todo, de modo que cuanto aparezca podrá presentarse después como un hallazgo casual que en realidad estaba preconstituido por la amplitud de la búsqueda; frente a una propuesta de esa índole, el juez debe exigir su acotamiento antes de que el examen comience. Así lo entendió la Corte de Apelaciones de Valparaíso en un amparo reciente, deducido por una imputada contra la negativa del juez de garantía a limitar el examen de los dispositivos que le fueron incautados, al ordenar que los descriptores de búsqueda fueran informados



al juzgado de garantía (SCA de Valparaíso rol 3810-2026, 1 de septiembre de 2026, confirmada por SCS rol 49.866-2026, 24 de septiembre de 2026, con declaración sobre las medidas a cargo del Ministerio Público).

Esos criterios han de aplicarse, ante todo, a las aplicaciones de mensajería, al correo electrónico y a las redes sociales, que son hoy el principal depósito de las comunicaciones de una persona y, previsiblemente, el objeto central del examen, y no sólo a los archivos que el aparato guarda en sus carpetas. Sus registros forman parte del contenido extraído, sea que estén almacenados en el dispositivo o que la aplicación los sincronice desde servidores remotos a través de la sesión abierta, según se dijo en el considerando décimo, y quedan sujetos a las mismas limitaciones. Respecto de ellos, la delimitación por cuenta, interlocutor y período es la que permite que el persecutor lea las conversaciones y los correos intercambiados con las personas y en la época que interesan a la investigación, y no la totalidad de los intercambios del amparado con quienes nada tienen que ver con ella, mientras que las palabras clave y las categorías de contenido cumplen esa función respecto de las conversaciones de grupo y de las casillas con numerosos remitentes. Las herramientas de análisis forense permiten filtrar los registros extraídos por contacto, cuenta, fecha y término de búsqueda, de modo que la limitación no es impracticable y, si el persecutor sostuviere lo contrario en algún caso, deberá justificarlo ante el juez.

Distinto es el caso de las fotografías, los videos y los audios. Su contenido no está expresado en texto, de modo que las palabras clave no permiten seleccionarlos; lo que sí permite acotar el universo son los datos asociados a cada archivo, esto es, la fecha en que se creó o recibió, el lugar en que se captó y la conversación, correo o cuenta de la que proviene. Por eso, respecto de estos archivos, la limitación opera a través del período y de la procedencia, y dentro del conjunto así delimitado no hay otro modo de saber si son pertinentes que verlos u oírlos, revisión directa que, por lo mismo, importa una intromisión mayor y exige, como compensación, que la practiquen sólo los funcionarios individualizados, que no se generen copias adicionales, que se deje constancia de los archivos que se conservan y que los restantes, entre ellos los de carácter personal y familiar y los relacionados con patrocinados o con otras causas, cuya exclusión el



recurso solicita, se eliminan con el excedente. Pretender que el persecutor identifique lo útil sin mirar sería tan ilusorio como permitirle mirar sin límite y sin registro.

La experiencia europea muestra el costo de omitir esas determinaciones. En *Särgava c. Estonia*, el Tribunal Europeo de Derechos Humanos constató que la orden de registro no previó resguardo alguno para el material protegido, que la búsqueda por palabras clave sobre la copia del teléfono y del computador de un abogado no derivaba de la ley ni de la orden, sino de una decisión de los propios investigadores, quienes eligieron términos tan amplios como “ejercicio financiero” o “línea de crédito”, y que el derecho interno no ofrecía mecanismo alguno para que el material disputado no llegara a los investigadores antes de que un tribunal lo analizara y, de ser necesario, ordenara su devolución o destrucción; por ello declaró violado el artículo 8 del Convenio. Y en *Nezirić c. Bosnia y Herzegovina* reiteró que copiar íntegramente el teléfono de un abogado y filtrar la copia con los números de los coimputados, sin que esa limitación proviniera de la ley ni estuviera sujeta a supervisión judicial, carece de las garantías procedimentales que exige el Convenio (TEDH, *Nezirić c. Bosnia y Herzegovina*, N° 4088/21, 5 de noviembre de 2024).

Décimo cuarto: Que, si el persecutor no ofrece esa delimitación, el juez debe exigirla y, en su defecto, establecerla. La cautela de garantías del artículo 10 del Código Procesal Penal lo faculta para adoptar, “de oficio o a petición de parte, las medidas necesarias” para permitir el ejercicio de los derechos del imputado, y el artículo 14 letra a) del Código Orgánico de Tribunales le encomienda “asegurar los derechos del imputado y demás intervinientes en el proceso penal”. En una diligencia que necesariamente pasa por la copia total del dispositivo, esas medidas consisten, cuando menos, en fijar un plazo para culminar la extracción y la identificación del contenido útil, en ordenar la eliminación del resto de la copia con certificación de haberse practicado y en resolver sobre la devolución del aparato o, si su conservación es necesaria, sobre su custodia. Nada de ello es ajeno a nuestro sistema. El deber de destruir las copias de lo impertinente ya está en el inciso cuarto del artículo 223 para las interceptaciones, y no se advierte razón para excluir de él a un registro que compromete la privacidad con mayor intensidad; la fijación de plazos y de



una duración precisa está en los artículos 222 y 225 ter; y la custodia de lo incautado, con acceso de los intervinientes autorizado por el fiscal o, en su caso, por el juez de garantía, en el artículo 188.

El Tribunal Constitucional Federal alemán llegó a la misma solución cuando admitió que, en el acceso a sistemas informáticos, es prácticamente inevitable obtener información antes de poder determinar si pertenece al núcleo de la vida privada; en tal caso, dijo, la protección debe asegurarse en la fase de análisis, mediante un procedimiento que examine los datos recogidos y disponga que los que pertenezcan a ese núcleo se eliminen sin dilación y no puedan utilizarse ni transmitirse (BVerfG, sentencia de 27 de febrero de 2008). En el ámbito del Convenio Europeo, el control judicial posterior fue la garantía decisiva en *Sérvulo & Asociados c. Portugal*, donde no se declaró violación porque el juez de instrucción revisó lo incautado en un estudio de abogados y ordenó destruir cerca de 850 archivos que contenían información personal, cubierta por el secreto profesional o relativa a personas no investigadas (TEDH, *Sérvulo & Asociados - Sociedade de Advogados, RL y otros c. Portugal*, N° 27013/10, 3 de septiembre de 2015). Y entre nosotros, el fallo de la Corte de Apelaciones de Valparaíso ya citado dispuso, además de la comunicación de los descriptors de búsqueda, que el Ministerio Público informara al tribunal los funcionarios con acceso a los dispositivos, dejara fuera del análisis lo impertinente y eliminara toda la información extraída fuera de esos límites, informando los protocolos seguidos y las personas encargadas. Al confirmarlo, la Corte Suprema declaró que los dispositivos incautados y su custodia deben quedar únicamente a cargo del fiscal responsable de la investigación, que el Ministerio Público debe informar al juez de garantía el nombre de los funcionarios que tendrán acceso a ellos, que no puede utilizarse información anterior a la época que fijó, que debe quedar fuera de análisis toda la información que carezca de pertinencia con los hechos que justificaron la incautación, a excepción de los hallazgos que puedan revestir caracteres de otros ilícitos, y que toda la información extraída fuera de esos límites, y de la que se hubieren hecho copias sin interés criminalístico, debe ser eliminada, informando al tribunal los protocolos seguidos y las personas encargadas de su ejecución. Recordó, asimismo, que el Código no sólo regula los casos y formas de la



interceptación, sino también, en el artículo 223, el destino de la información obtenida, como lo hace el inciso final del artículo 218 para la correspondencia.

Décimo quinto: Que la determinación del objeto tiene otra consecuencia, referida a los hallazgos que se produzcan durante la revisión. El artículo 215 del Código Procesal Penal permite incautar los objetos o documentos que, durante la práctica de un registro, hagan sospechar la existencia de un hecho punible distinto. Esa regla se concibió para la entrada y registro en lugares cerrados, donde las divisiones físicas permiten deslindar lo autorizado de lo que no lo está. En el interior de un teléfono no hay habitaciones ni cajones que separen unos contenidos de otros; todo está al alcance del mismo examen. Si bastara, entonces, con que un contenido apareciera durante la revisión para autorizar su uso, la orden que recae sobre un teléfono se convertiría en una orden sobre todo el teléfono, y la determinación de su objeto perdería todo sentido. La doctrina ha advertido que, conforme al principio de especialidad, no es admisible una incautación destinada a descubrir, sin la adecuada precisión, actos delictivos cualesquiera, lo que convertiría la orden en una autorización en blanco, y que admitir el hallazgo casual sin límites llevaría a que “cualquier incautación de un dispositivo informático se transforme en una búsqueda general, habilitada para capturar cualquier evidencia de cualquier delito” (Núñez Ojeda, R., Beltrán Calfurrapa, R. y Santander Akkrass, N., *ob. cit.*, pp. 173 y 180; en el mismo sentido, pp. 176-177).

De ahí que el persecutor no pueda servirse de la copia para revisar el teléfono en busca de otros delitos. Si la orden no fija límites a la revisión, todo lo que aparezca en la copia será, por definición, encontrado “casualmente”, y la excepción del hallazgo casual, pensada para lo que surge sin buscarlo, terminará por cubrir lo que la orden debía impedir, esto es, la revisión exploratoria de todo el contenido en busca de algún delito, sin saber cuál, que la doctrina y la jurisprudencia comparadas llaman investigación prospectiva. Con límites, en cambio, el hallazgo es casual sólo cuando se produce de manera inevitable en el curso de la ejecución legítima de la orden y dentro de ellos; cuando la revisión se extiende deliberadamente a contenidos que la orden no cubría, lo encontrado no es fruto del azar, sino de una desviación de la orden judicial que no puede



aprovecharse. Es al Ministerio Público a quien corresponde acreditar que la ejecución de la orden, respetado el principio de especialidad, conducía necesariamente a la información del delito distinto, porque es él quien conduce el examen, quien está en condiciones de registrar cómo se practicó y sobre quien pesa el deber de fundamentar sus actuaciones. Esta Corte ya advirtió, al conocer de una acción de protección referida a la transcripción de centenares de miles de páginas de mensajería extraídas de un teléfono, que la orden judicial sólo pudo referirse a las conversaciones relacionadas con el objeto de la investigación y que es deber del Ministerio Público cautelar, en su labor, los derechos constitucionales de los terceros ajenos a ella (SCA de Santiago rol 6423-2024, 28 de junio de 2024); y el voto de minoría de ese fallo, que estuvo por acoger la acción, precisó que el persecutor no puede, sin incurrir en ilegalidad, hurgar en esas transcripciones en una suerte de búsqueda de ilícitos ajenos al objetivo de la orden judicial, pues el orden correcto es el inverso, esto es, iniciar una investigación por un delito determinado y, según los datos que ella arroje, solicitar la autorización para develar los mensajes, sin que la autorización otorgada constituya “una especie de patente de corso” para buscar y rebuscar en ellas algún ilícito distinto del que inició la investigación. Cuando, en el curso de la revisión legítima, aparezca información sobre otro hecho punible, lo procedente será ponerla en conocimiento del juez de garantía y obtener de él la autorización para utilizarla, con el umbral de gravedad que el inciso final del artículo 223 fija para la información obtenida en una interceptación, analogía que se impone por la equivalente intensidad de ambas injerencias, en lugar de acudir a la más laxa del artículo 215, pensada para un continente físico.

Ese control se ejerce después de la revisión y tiene un objeto preciso. Corresponde al juez que autorizó la diligencia, aunque la investigación del nuevo delito llegue a radicarse ante otro tribunal, porque es él quien fijó los límites de la orden y recibió los criterios de búsqueda, de modo que sólo él está en condiciones de cotejar lo hecho con lo autorizado y de verificar que su orden no haya sido excedida bajo la apariencia de un hallazgo; así ocurre en las medidas intrusivas que la ley regula, en que el mismo juez que las autoriza examina cada vez la subsistencia de sus requisitos para prorrogarlas, y así lo dispone el inciso cuarto del artículo 220 cuando



entrega al juez, a la vista de los objetos, la decisión sobre la legalidad de la incautación. Dejar esa verificación para el tribunal de la causa nueva significaría que el Ministerio Público podría invocar siempre un hallazgo casual y diferir el control a un juez que sólo intervendría si esa otra investigación prospera, conservando entretanto la información privada y eludiendo los resguardos aquí descritos. Cuando el Ministerio Público invoque un hallazgo, deberá explicar ante el juez que autorizó la diligencia con qué descriptor, palabra clave, interlocutor o filtro llegó a la información de que se trata, y el tribunal apreciará si esa búsqueda era razonable en relación con el objeto autorizado y con los criterios comunicados, en cuyo caso el hallazgo será casual y podrá autorizar su uso, o si se trató de una revisión exploratoria que ninguno de esos criterios justificaba, o de criterios tan amplios que la revisión abarcó en los hechos todo el contenido, en cuyo caso la información se obtuvo fuera de los supuestos que la ley admite, no podrá utilizarse en esta ni en otra investigación y deberá eliminarse junto con el excedente de la copia. No se trata de anticipar el debate sobre exclusión de prueba de la audiencia de preparación del juicio oral, que conserva su ámbito respecto de lo que se ofrezca como evidencia en esta causa, sino de controlar la ejecución de una orden intrusiva, tarea que pertenece al juez que la dictó. Autorizado el uso, la investigación del hecho distinto seguirá su curso ante el tribunal que corresponda. El derecho comparado conoce, a título ilustrativo, exigencias semejantes, pues la Ley de Enjuiciamiento Criminal española sólo permite utilizar en otro proceso la información obtenida en una medida de investigación tecnológica dejando constancia de la solicitud inicial, de la resolución que la acordó y de sus prórrogas, y somete la continuación de la medida respecto del delito casualmente descubierto a un nuevo control judicial, según sus artículos 579 bis y 588 bis i.

Décimo sexto: Que las medidas descritas no suponen que el juez de garantía se entrometa en la investigación ni que determine qué información es útil para ella, decisión que el artículo 3° del Código Procesal Penal y el artículo 83 de la Constitución reservan al Ministerio Público. El juez no selecciona la prueba; fija las condiciones bajo las cuales una diligencia que él autorizó puede ejecutarse sin afectar más de lo necesario los derechos del imputado y de terceros, que es la función que el artículo 14 letra a) del



Código Orgánico de Tribunales le asigna. No es extraño a nuestro sistema que el juez oriente de ese modo la ejecución de una diligencia. El legislador, al regular el registro remoto de equipos informáticos, exige que la resolución que lo autoriza especifique “la forma en la que se procederá al acceso y aprehensión de contenidos relevantes para la causa”, según la letra b) del artículo 225 ter, forma que el fiscal propone en su solicitud y que el juez fija y controla, sin que nadie haya visto en ello una intromisión en la dirección de la investigación. La Corte Suprema ha destacado la importancia de establecer altos estándares de exigencia respecto de la actuación de los sujetos procesales en las primeras diligencias del procedimiento, “siendo una función esencial del Juez de Control adoptar las medidas necesarias que permitan la protección y el ejercicio de las garantías que la Constitución, las Leyes y los Tratados Internacionales otorgan a todas las personas” (SCS rol 14.900-2024, 9 de mayo de 2024). El juez que autoriza una intromisión no puede, por lo mismo, desentenderse de sus efectos. La Corte Suprema lo ha dicho al confirmar el fallo de la Corte de Valparaíso ya citado: no basta con que la judicatura haya autorizado al Ministerio Público para que la afectación del derecho sea legítima, pues “una comprensión tan acotada de la intervención judicial equivaldría a una delegación de sus facultades jurisdiccionales” y a una vulneración del mandato constitucional de reserva de ley para la afectación justificada y proporcional del derecho (SCS rol 49.866-2026, 24 de septiembre de 2026).

Tampoco altera esta conclusión la autonomía que el artículo 83 de la Constitución reconoce al persecutor, invocada en el informe. Esa misma norma dispone que las actuaciones que priven al imputado o a terceros del ejercicio de los derechos que la Constitución asegura, o los restrinjan o perturben, requieren de aprobación judicial previa, de modo que la intervención del juez en la delimitación de tales actuaciones no es una injerencia en la dirección de la investigación, sino el presupuesto constitucional de su legitimidad. Dirigir la investigación es decidir qué se investiga y con qué diligencias; señalar los términos en que una de ellas puede afectar la privacidad de las personas es tarea del tribunal. Por eso la Corte de Apelaciones de Valparaíso pudo observar, en el precedente citado, que el equilibrio entre los derechos de la imputada y las prerrogativas del Ministerio Público exige protocolos preestablecidos y rigurosos en el



examen y traspaso de la información contenida en los dispositivos, y que su mayor especificación por la judicatura, “que es la primera llamada a asegurar el pleno respeto de las garantías de los intervinientes”, no debiera causar inquietud al persecutor.

Décimo séptimo: Que el silencio del Código Procesal Penal sobre el vaciado y revisión de teléfonos, computadores y otros equipos incautados no priva al juez de esas atribuciones ni deja la diligencia sin límites; significa sólo que éstos deben construirse desde los principios que gobiernan a todas las medidas intrusivas, esto es, la autorización judicial previa del artículo 9°, la interpretación restrictiva del artículo 5° y la fundamentación del artículo 36, y desde la facultad que el artículo 10 confiere al juez para adoptar de oficio las medidas necesarias en cautela de las garantías. El Tribunal Europeo de Derechos Humanos, ante la ausencia de una regulación específica del acceso policial al contenido de un computador, ha exigido igualmente que el derecho interno, integrado por la jurisprudencia, imponga la autorización judicial previa y un control judicial efectivo, y ha declarado violado el Convenio cuando el examen íntegro de los archivos se practicó sin ella y sin urgencia que lo justificara (TEDH, Trabajo Rueda c. España, N° 32600/12, 30 de mayo de 2017).

Décimo octavo: Que el control descrito exige, además, una oportunidad para ejercerlo. La orden que autoriza la extracción debe señalar desde ya la audiencia en que se verificará su cumplimiento, en particular para disponer la destrucción del excedente de la copia y resolver sobre la devolución o custodia del aparato, del mismo modo que la interceptación y el registro remoto tienen una duración precisa y una prórroga sujeta a nuevo examen judicial. No basta con remitir la cuestión a la audiencia de preparación del juicio oral, como hace la resolución recurrida. La exclusión probatoria sólo operaría si el persecutor decide usar la información, en un procedimiento que puede no llegar a esa etapa y que en nada resguarda a los terceros, que no son intervinientes y jamás sabrán que sus comunicaciones fueron revisadas; y, entretanto, ni el imputado ni esos terceros tienen por qué soportar, sin una justificación que la ley no ofrece, que un órgano del Estado conserve durante meses o años, en una copia sobre la que ningún tribunal ejerce control, información sobre sus vidas que no guarda relación con el delito investigado. La retención de esos datos es



por sí misma una injerencia que se prolonga en el tiempo, y no un mero antecedente de la que se produciría al usarlos; por eso el inciso cuarto del artículo 223 no espera al juicio para ordenar la destrucción de las copias de lo impertinente, y por eso los tribunales citados en el considerando décimo cuarto sitúan la eliminación inmediatamente después del examen y cuentan la injerencia desde la incautación hasta la destrucción. Una investigación de la envergadura de la presente puede prolongarse largamente antes de que se formule acusación, si es que se formula, y durante todo ese lapso, sin las medidas que aquí se disponen, el contenido íntegro del teléfono permanecería a disposición del persecutor.

Décimo noveno: Que los instructivos del Ministerio Público a los que remite la resolución recurrida no bastan para conjurar la afectación descrita. El Oficio FN N° 983/2024 constituye, según sus propios términos, “normativa interna del Ministerio Público”; se aplica sólo a las causas complejas que el fiscal regional decida someter a él; confía al fiscal la evaluación inicial acerca de si la información es o no sensible y de interés investigativo; le permite considerar que toda la información de la carpeta es de interés investigativo, no sujeta a regla de protección; radica en él la decisión de anexar lo impertinente, que no se elimina sino que se guarda en custodia con un número único de evidencia, y prevé que el mismo fiscal puede reincorporarlo a la carpeta cuando surjan nuevas líneas de indagación. El Oficio FN N° 363/2025, por su parte, ordena a los fiscales instruir a las policías que excluyan de los informes policiales la información de la vida privada penalmente irrelevante y, si el informe la incluye, pedir una audiencia para que tales antecedentes queden reservados. Ninguno de los dos contempla la eliminación del excedente de la copia forense, ni plazos, ni un control judicial en una oportunidad determinada; la información privada e impertinente queda, en todos los casos, en poder del persecutor y bajo su exclusiva apreciación.

La misma jueza recurrida reconoció que esos instructivos dejan a salvo sólo “varias de las aprehensiones” de los litigantes y se mostró dispuesta a complementar lo resuelto para limitar o aclarar su alcance, lo que confirma que la protección quedó incompleta. Los criterios internos de actuación son valiosos, pero no sustituyen la garantía judicial, porque la decisión sobre el alcance de una injerencia en derechos fundamentales no



puede quedar entregada al órgano que la ejecuta y tiene interés en su resultado. En *Särgava c. Estonia* el Tribunal Europeo estimó insuficiente que el filtrado de la copia hubiera quedado enteramente en manos de las autoridades investigadoras, y en *Nezirić c. Bosnia y Herzegovina* no bastó que los investigadores hubieran actuado concienzudamente y tratado los datos como secreto oficial, porque la búsqueda selectiva no derivaba de la ley y se practicó sin supervisión judicial. La Corte Suprema estadounidense, en fin, frente a la propuesta del Gobierno de que las agencias desarrollaran protocolos para resolver los problemas del acceso a los datos del teléfono, observó que probablemente era una buena idea, pero que los fundadores no habían combatido una revolución para obtener el derecho a los protocolos de las agencias gubernamentales (*Riley v. California*, 573 U.S. 373, 398).

Vigésimo: Que no cabe acoger, en cambio, la pretensión de que un ministro de fe de esta Corte, un juez de garantía distinto o un tercero independiente determinen qué información contenida en el teléfono es útil para la investigación. En nuestro sistema esa apreciación corresponde únicamente al Ministerio Público, que dirige en forma exclusiva la investigación conforme a los artículos 83 de la Constitución y 3° del Código Procesal Penal y que, además, cuenta con los medios técnicos y la capacidad de análisis para efectuarla. El ordenamiento no contempla un tercero independiente que pueda intervenir en el proceso penal y acceder al material de la investigación, y su intervención sería aún menos concebible en una indagación reservada como la presente, sujeta al secreto que el artículo 31 de la Ley N° 19.913 impone, según se consignó en la audiencia. Lo que el juez puede y debe hacer es fijar los límites de la búsqueda, recibir del persecutor los criterios con que la practicará, apreciar si son razonables y controlar después su cumplimiento, no ejecutarla ni sustituir al persecutor en la selección de la evidencia. Tampoco se trata, como temió la recurrida, de dejar la entrega de la información al arbitrio de la persona investigada, pues los criterios los propone el persecutor y los aprueba el juez, sin que el imputado intervenga en su definición.

Vigésimo primero: Que, asimismo, no procede la prohibición absoluta de acceso a toda comunicación amparada por el secreto profesional que el recurrente solicita en primer término, ni el artículo 220 del



Código Procesal Penal, en que la funda, ofrece la solución del caso. Esta norma impide incautar las comunicaciones entre el imputado y las personas que pueden abstenerse de declarar por parentesco, conforme al artículo 302, o por razón de secreto, conforme al artículo 303, así como las notas y documentos a que se extiende esa facultad, pero su inciso segundo dispone que esas limitaciones “sólo regirán” cuando tales objetos “se encontraren en poder de las personas a quienes la ley reconoce la facultad de no prestar declaración”, y las extiende a las oficinas o establecimientos de los profesionales del artículo 303. La norma protege, entonces, la confianza que el imputado deposita en su pariente, su abogado, su médico o su confesor, y lo hace impidiendo que lo confiado se incaute en manos de estos últimos; su ámbito propio sería el teléfono, el dispositivo o los papeles del abogado defensor del amparado, en los que constaran las consultas o la asesoría de su defensa, y no el caso de autos, en que lo incautado es el teléfono del imputado mismo, pues la norma no establece una prohibición general de incautar sus comunicaciones dondequiera que se encuentren. A ello se agrega que el inciso tercero excluye las limitaciones cuando las personas facultadas para no prestar testimonio fueren imputadas por el hecho investigado, de modo que, aun si el teléfono del amparado se mirara como el archivo profesional de un abogado y sus clientes fueran los imputados cuya confianza se resguarda, la protección cedería igualmente, por revestir el propio abogado la calidad de imputado, como lo resolvió la recurrida. Otro tanto cabe decir de los tratados que el recurso invoca, pues los artículos 8.2 letra d) de la Convención Americana sobre Derechos Humanos y 14.3 letra b) del Pacto Internacional de Derechos Civiles y Políticos aseguran a quien es inculcado el derecho a comunicarse con el defensor de su elección, libre y privadamente en los términos de la primera, y no una inmunidad del abogado que es investigado respecto de sus propios dispositivos.

Descartado que el artículo 220 sea aplicable al caso de autos, y para mayor claridad de lo que se resolverá, conviene entonces distinguir tres situaciones.

La primera es la de las comunicaciones que el amparado, en cuanto imputado, haya mantenido con sus abogados defensores, en esta o en otras causas judiciales, para preparar y ejercer su defensa. Están protegidas, aunque no específicamente por el artículo 220, sino por el derecho a la



defensa que aseguran el artículo 19 N° 3 de la Constitución y el artículo 8° del Código Procesal Penal, y por la misma razón que lleva al inciso tercero del artículo 222 a prohibir la interceptación de las comunicaciones entre el imputado y su abogado, salvo que el juez estime fundadamente que éste pudiere tener responsabilidad penal en los hechos investigados. Por eso, si el aparato las contiene, deben quedar excluidas de la búsqueda y eliminarse de la copia, aun cuando los criterios de búsqueda las alcancen, a menos que el abogado de que se trate sea también imputado por los hechos investigados, circunstancia que ni siquiera se ha mencionado en esta causa.

La segunda es la de las comunicaciones con los clientes a quienes asistió como abogado, con los antecedentes de víctimas que dice conservar bajo la reserva del artículo 15 de la Ley N° 19.992, en asuntos ajenos a los hechos investigados. Su protección, como se dijo, no proviene del artículo 220, cuya aplicación supondría que esos clientes o representados fueran imputados, calidad -huelga explicar- que no tienen. Por ello, la protección de esos terceros, más allá del secreto profesional, que sólo alcanzaría a una parte de lo que el aparato contiene, reside más bien en la garantía que los numerales 4° y 5° del artículo 19 de la Constitución dispensan a toda comunicación y a toda forma de vida privada, del amparado y de esos terceros, respecto de información que, según la propia recurrida, no guarda relación con los hechos investigados. Ese criterio, la impertinencia de la información, cubre por igual las comunicaciones con clientes, familiares, amigos o cualquier otra persona, es el que subyace a lo dicho en el considerando noveno y justifica que se ordene excluirlas de la búsqueda y eliminarlas de la copia.

La tercera es la de las comunicaciones con esas mismas personas que sí se relacionan con los delitos investigados. No cabe excluirlas de antemano en bloque, porque los criterios de búsqueda, determinados por los hechos, las personas y la época de interés, pueden conducir a intercambios que el amparado sostuvo con un cliente, un representado o un pariente y que conciernen a esos hechos; si quedan comprendidas en esos criterios, y dado que el amparado es imputado, tales comunicaciones son pertinentes, y la facultad de abstenerse de declarar que los artículos 302 y 303 reconocen al pariente o al profesional no crea, sobre los registros que el imputado guarda en su teléfono, una zona inmune a la investigación que se



sigue en su contra, de suerte que pueden ser examinadas, conservadas y utilizadas.

Por último, no cabe aplicar por analogía el mecanismo del inciso cuarto del artículo 220, que ante la duda sobre la procedencia de la incautación permite al juez ordenarla y examinar él mismo los objetos, sin intervención previa del fiscal ni de la policía, para decidir sobre la legalidad de la medida y ordenar la devolución de lo protegido. Ese examen recae sobre elementos objetivos, como si el tenedor es una persona exenta de declarar, si el documento es un diagnóstico médico o una nota tomada por el abogado sobre lo que su cliente le confió, y por eso puede confiarse al juez a la vista de los objetos; nada tiene en común con determinar si una conversación, una fotografía o un archivo son útiles para una investigación, juicio que exige conocer la hipótesis delictiva y los antecedentes reunidos y que pertenece al persecutor. En lo que la resolución recurrida acertó fue en señalar que indagar en las comunicaciones del amparado con sus clientes no es parte de la investigación, con lo que se hizo cargo del secreto profesional invocado, contra lo que el recurso le reprocha; lo que faltó fue hacer efectivo ese resguardo con medidas concretas.

Vigésimo segundo: Que lo que se resolverá no busca limitar ni obstaculizar la investigación del Ministerio Público, sino alcanzar el equilibrio entre la eficacia de la persecución penal y el respeto de los derechos fundamentales que la Constitución exige en toda diligencia intrusiva. La extracción y el análisis del contenido del teléfono podrán continuar; la delimitación de los hechos, del período y de las personas de interés seguirá siendo propuesta por el persecutor; y ningún antecedente pertinente a los hechos investigados quedará fuera de su alcance. Lo único que se agrega es aquello que el legislador ya impone a diligencias de intensidad comparable, esto es, un plazo, un objeto determinado, la destrucción de lo que no sirve y una oportunidad para que el juez verifique que así se hizo. Ese es el sentido del artículo 10 del Código Procesal Penal cuando faculta al juez para adoptar las medidas necesarias para el ejercicio de las garantías, y del artículo 14 letra a) del Código Orgánico de Tribunales cuando le encomienda asegurarlas. Esta Corte no desconoce que se trata de un control que los tribunales no han practicado, o sólo excepcionalmente, respecto de una diligencia que la ley no regula. Por eso las medidas que se



adoptan son las que parecen razonables y prudentes para restablecer el equilibrio buscado, en la expectativa de que resulten suficientes; pero, dada la dificultad de la materia, el mismo juzgado de garantía podrá revisarlas, de oficio o a petición de cualquier interviniente, cuando su ejecución muestre que son insuficientes para proteger los derechos comprometidos o que entorpecen innecesariamente la investigación, y hacer los ajustes que ese equilibrio requiera.

Vigésimo tercero: Que, conforme a lo razonado, la resolución de 26 de agosto de 2026, en cuanto rechazó fijar límites a la ejecución de la extracción y revisión del teléfono del amparado más allá de los que consignó, y remitió el resguardo de la información impertinente y privada a instructivos internos del persecutor y a una eventual exclusión probatoria futura, no satisfizo las exigencias que los artículos 5°, 9°, 10 y 36 del Código Procesal Penal y 14 letra a) del Código Orgánico de Tribunales imponen al juez de garantía, y dejó subsistente una afectación cierta y actual de la vida privada del amparado y de la inviolabilidad de sus comunicaciones y de las de terceros, sobre la cual, conforme a lo resuelto por la Corte Suprema, corresponde a esta Corte pronunciarse derechamente, y que debe hacer cesar. En un caso semejante, el máximo tribunal ha estimado que exponer a la imputada a pesquisas investigativas sin la adopción de medidas de contrapeso que resguarden sus garantías fundamentales amenaza indebidamente su libertad personal y afecta de manera ostensible su derecho a la intimidad (SCS rol 49.866-2026, 24 de septiembre de 2026). Las medidas que se dispondrán siguen las líneas de ese precedente, con el apoyo que la regla del inciso cuarto del artículo 223 presta a la eliminación del excedente de la copia, y agregan la fijación de un plazo y de una audiencia de control. La identificación de la información útil deberá completarse dentro de noventa días contados desde la notificación de esta sentencia, plazo que sólo podrá ampliarse por una vez, por resolución fundada dictada en audiencia, para que por esa vía no se eluda el control ni se prolongue la conservación de la copia; y la audiencia en que se verificará lo obrado y se dispondrá la eliminación se celebrará dentro de los diez días siguientes, con citación de la defensa del amparado. La reserva de la investigación decretada con arreglo al artículo 31 de la Ley N° 19.913 no es obstáculo para ello. Esa norma permite mantener en secreto la investigación



respecto del imputado, pero la audiencia versará sobre la conservación de la copia del contenido de su propio teléfono, que él obviamente conoce, y sobre los descriptors con que se acota la búsqueda y la información que se estima impertinente, cuya revelación no compromete de modo relevante el secreto ni el éxito de la investigación, menos aún cuando los delitos que se indagan constan en los escritos públicos de este amparo y las defensas conocen los hechos desde la audiencia de cautela de garantías. Diferir el control hasta el término de la reserva, que puede extenderse por un año, sería una forma de eludirlo. Durante ese plazo el persecutor y la policía trabajarán sobre la copia íntegra para identificar lo pertinente; completada la identificación, y hasta que la audiencia resuelva sobre la eliminación, la copia quedará sellada y sin acceso, porque desde ese momento el examen ha concluido y el persecutor sólo necesita la información que separó como relacionada con los hechos, de modo que en el lapso que media entre el término del examen y la audiencia la retención deja de ser una intromisión en curso.

Así, el amparo será acogido sólo en cuanto se dispondrán las medidas de control que se indicarán, y rechazado en lo demás, sin costas.

Por estas consideraciones y de conformidad, además, con lo dispuesto en el artículo 21 de la Constitución Política de la República y en el Auto Acordado de la Excma. Corte Suprema sobre Tramitación y Fallo del Recurso de Amparo, **se acoge**, sin costas, el recurso de amparo deducido por Hugo Humberto Gutiérrez Gálvez, en su propio favor, en contra del Cuarto Juzgado de Garantía de Santiago, sólo en cuanto se declara que la resolución dictada el 26 de agosto de 2026 en la causa RUC 2600858361-6, RIT O-6719-2026, debe complementarse con las siguientes medidas, que dicho tribunal deberá adoptar y controlar:

a) El Ministerio Público informará al Cuarto Juzgado de Garantía de Santiago, dentro de quince días, el estado de la extracción y de la revisión ya practicada, la individualización de los funcionarios y peritos que han tenido y tendrán acceso a la copia obtenida del teléfono del amparado, y propondrá los criterios de búsqueda con que se practicará el análisis de la totalidad de lo extraído, incluidas las comunicaciones de las aplicaciones de mensajería, del correo electrónico y de las redes sociales, sean palabras clave, interlocutores, cuentas, tipos de archivo u otros descriptors,



determinados por los hechos investigados, por el período comprendido entre el año 2018 y el 20 de agosto de 2026 ya fijado en la resolución recurrida y por las personas, números o cuentas de interés para la investigación, sin perjuicio de su posterior complementación con conocimiento del tribunal. Esos criterios excluirán las comunicaciones y documentos relativos a los clientes del amparado en el ejercicio de su profesión de abogado en asuntos ajenos a los hechos investigados, sin perjuicio de que las comunicaciones alcanzadas por los criterios de búsqueda, por relacionarse con esos hechos, puedan ser examinadas y conservadas cualquiera sea su interlocutor; si el Ministerio Público tuviere antecedentes para estimar que en las comunicaciones excluidas hay también elementos útiles para la investigación de los delitos de esta causa, deberá justificarlo determinadamente ante el juez de garantía, quien resolverá. Quedarán excluidas de la búsqueda, y serán eliminadas de la copia, las comunicaciones del amparado con sus abogados defensores, en esta o en otras causas, relativas al ejercicio de su defensa, a menos que el abogado respectivo fuere imputado por los hechos investigados. El juez de garantía apreciará la precisión y razonabilidad de los criterios propuestos y podrá exigir su acotamiento. El teléfono incautado y las copias obtenidas de él permanecerán bajo la custodia exclusiva del fiscal adjunto a cargo de la investigación.

b) La identificación de la información útil para la investigación deberá completarse dentro de noventa días contados desde la notificación de esta sentencia. El juez de garantía podrá ampliar ese plazo por una sola vez, por resolución fundada dictada en audiencia a la que se citará a la defensa del amparado, previo informe del Ministerio Público sobre el estado de la diligencia; la ampliación no suspenderá las demás medidas de esta sentencia. Vencido el plazo o su ampliación, el Ministerio Público separará en un soporte distinto la información identificada como relacionada con los hechos investigados e informará de ello al tribunal, y la copia íntegra del aparato quedará desde entonces sellada, bajo la custodia del fiscal a cargo conforme al artículo 188 del Código Procesal Penal, sin acceso alguno hasta que el tribunal resuelva sobre su eliminación.

c) Dentro de los diez días siguientes al vencimiento del plazo de la letra b) o de su ampliación, el Cuarto Juzgado de Garantía de Santiago



celebrará una audiencia, con citación de la defensa del amparado, en la que el Ministerio Público dará cuenta de la información que conservará por tener relación con los hechos investigados, incluida, en su caso, la obtenida a través de las cuentas abiertas en el teléfono a que se refiere la letra f), y en la que el tribunal dispondrá la eliminación de la copia íntegra sellada y de toda otra información extraída que no haya sido identificada como pertinente, en particular la relativa a los clientes del amparado a que se refiere la letra a), de lo que deberá dejarse constancia mediante certificación que identifique el procedimiento seguido y a los funcionarios que lo practicaron, y resolverá sobre la devolución del teléfono al amparado o, si su conservación fuere necesaria, sobre su custodia. La reserva de la investigación decretada conforme al artículo 31 de la Ley N° 19.913 no suspenderá esta audiencia ni la intervención de la defensa del amparado en ella.

d) Hasta que se celebre esa audiencia, el Ministerio Público podrá utilizar en la investigación únicamente la información que identifique como relacionada con los hechos investigados. La información restante no podrá ser examinada más allá de lo necesario para su identificación, ni entregada a otros intervinientes o a terceros, ni incorporada a la carpeta investigativa ni a informes policiales, conforme a lo ya resuelto por el tribunal recurrido, y quedará comprendida en la copia sellada a que se refiere la letra b).

e) Si el Ministerio Público estimare que la copia contiene información relevante para hechos distintos de los investigados, deberá ponerlo en conocimiento del Cuarto Juzgado de Garantía de Santiago antes de utilizarla con cualquier fin, indicando el criterio o descriptor de búsqueda con que llegó a ella. El tribunal, con los criterios informados conforme a la letra a), verificará si se trató de un hallazgo casual, producido dentro de los límites de la orden y de una búsqueda razonable, y no de una revisión exploratoria del contenido en busca de delitos no determinados. Si lo estima así, autorizará su uso; en caso contrario, la información no podrá utilizarse en esta ni en otra investigación y será eliminada junto con el excedente de la copia conforme a la letra c). En caso de urgencia, la autorización podrá requerirse por la vía más rápida.

f) Las limitaciones anteriores rigen respecto de la totalidad de la información extraída, y en particular respecto de las aplicaciones de



mensajería, del correo electrónico y de las redes sociales, que concentran las comunicaciones del amparado. Los criterios de búsqueda de la letra a) deberán determinar, para cada una de ellas, las cuentas, los interlocutores o contactos y el período cuyas comunicaciones podrán examinarse, y las palabras clave o categorías de contenido a que se acotará la revisión, sin que puedan examinarse íntegramente conversaciones, casillas o perfiles de personas ajenas a los hechos investigados. Esas mismas limitaciones se aplican a la información que no está grabada en el teléfono, sino almacenada en los servidores de esos servicios o en los de almacenamiento en la nube, y a la que el aparato permite ingresar directamente por mantener abierta la sesión de la cuenta respectiva, acceso que la resolución de 19 de agosto de 2026 autorizó en términos genéricos; a su respecto, el Ministerio Público informará además al tribunal, en el plazo de la letra a), a qué servicios y cuentas ha accedido o pretende acceder por esa vía, para que el juez de garantía determine el alcance de ese acceso con arreglo a los artículos 225 bis y 225 ter del Código Procesal Penal, y fuera de lo así informado y autorizado no podrá ingresarse a esos servicios a través de las cuentas abiertas en el aparato.

g) Las fotografías, videos y audios contenidos en el aparato o accesibles a través de las cuentas abiertas en él, cuyo contenido no puede seleccionarse mediante palabras clave, se examinarán con sujeción al período fijado y a su procedencia, ordenando la revisión a partir de los archivos adjuntos a las conversaciones, correos o cuentas comprendidos en los criterios de búsqueda. Dentro de ese universo la revisión será directa y la practicarán únicamente los funcionarios individualizados conforme a la letra a), sin generar copias adicionales, dejando constancia de los archivos que se conserven por su relación con los hechos investigados; los restantes, incluidos los de carácter personal y familiar, quedarán comprendidos en la eliminación de la letra c).

h) El Cuarto Juzgado de Garantía de Santiago podrá, de oficio o a petición de cualquier interviniente y por resolución fundada dictada en audiencia, ajustar las medidas anteriores cuando su ejecución muestre que resultan insuficientes para resguardar los derechos comprometidos o que entorpecen innecesariamente la investigación.

Regístrese, notifíquese y archívese.



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: FMYDXKZUUP

Redacción del ministro Manuel Rodríguez Vega.

N° Amparo-4262-2026.

No firma la ministra señora Rodríguez Fondón, no obstante haber concurrido a la vista y al acuerdo del fallo, por estar haciendo uso del permiso del artículo 347 del Código Orgánico de Tribunales.

 Manuel Esteban Rodríguez Vega Ministro Corte de Apelaciones Veintinueve de septiembre de dos mil veintiséis 13:08 UTC-3   Carolina Sandra Brengi Zunino Ministro Corte de Apelaciones Veintinueve de septiembre de dos mil veintiséis 13:04 UTC-3 



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: FMYDXKZUUP

Pronunciado por la Sexta Sala de la C.A. de Santiago integrada por los Ministros (as) Manuel Esteban Rodríguez V., Carolina S. Brengi Z. Santiago, veintinueve de septiembre de dos mil veintiseis.

En Santiago, a veintinueve de septiembre de dos mil veintiseis, notifiqué en Secretaría por el Estado Diario la resolución precedente.



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: FMYDXKZUUP

Santiago, veintinueve de septiembre de dos mil veintiséis.

Vistos y teniendo presente:

Primero: Que comparecen Alejandro Espinoza Bustos e Ignacio Sotomayor Uribe, abogados, en representación de Sergio Alfredo Gahona Salazar, Senador de la República, e interponen acción constitucional de amparo en su favor y en contra del Cuarto Juzgado de Garantía de Santiago, por dos resoluciones dictadas en la causa RUC 2600858361-6, RIT O-6719-2026. La primera es la de 19 de agosto de 2026, dictada por la jueza Francis Patricia Fell Franco, que autorizó diligencias intrusivas en contra del amparado, a juicio de los recurrentes sin fundamentación suficiente y sin delimitar el acceso del Ministerio Público y de las policías al contenido de las especies incautadas. La segunda es la de 26 de agosto de 2026, dictada por la jueza Daniela Verónica Guerrero González en la audiencia de cautela de garantías, que negó a la defensa el acceso a la solicitud del Ministerio Público en que se fundó aquella autorización, impidiéndole conocer la imputación y los antecedentes invocados para obtenerla, y rechazó circunscribir el objeto y el alcance de la revisión de los dispositivos incautados, permitiendo un examen que excede lo vinculado con los hechos investigados.

Sostienen que ambas resoluciones son ilegales, porque infringen los artículos 5° inciso segundo, 9°, 36, 218 y 220 del Código Procesal Penal, y que privan a la defensa de la posibilidad de controlar la legalidad y proporcionalidad de las diligencias intrusivas decretadas, con lo que amenazan la libertad personal del amparado, pues sirven de sustento a una persecución penal por delitos de cohecho, soborno, revelación de secreto, tráfico de influencias y lavado de activos, que contemplan penas privativas de libertad, y vulneran además su derecho a defensa y a una investigación racional y justa, su vida privada y la inviolabilidad de sus comunicaciones privadas, que aseguran los numerales 3°, 4° y 5° del artículo 19 de la Constitución Política de la República, así como los artículos 8 y 11 de la Convención Americana sobre Derechos Humanos y 14 y 17 del Pacto Internacional de Derechos Civiles y Políticos.

En cuanto a los hechos, exponen que el amparado fue intendente de la Región de Coquimbo, diputado por esa región durante dos períodos y es actualmente Senador de la República por esa misma región. El 20 de



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: QWDJDZLUUP

agosto de 2026, funcionarios de la Policía de Investigaciones practicaron una diligencia de entrada y registro en su oficina del edificio del ex Congreso Nacional, en Santiago, e incautaron diversos dispositivos personales y profesionales, entre ellos su teléfono celular y su computador. En esa oportunidad se le exhibió la resolución de 19 de agosto de 2026, que no contenía autorización para ingresar a esa oficina, de lo que dejó constancia al firmar el acta, y sólo después de la audiencia de 26 de agosto se entregó a la defensa una constancia de la autorización verbal de ingreso y registro, sin la firma de la magistrada que la habría otorgado, lo que le impide verificar su autenticidad. Añaden que la resolución de 19 de agosto se remite de modo genérico a los antecedentes contenidos en la solicitud de la fiscal y en anteriores solicitudes del Ministerio Público, sin precisar los hechos, los delitos ni la época que se atribuyen al amparado, y que no delimitó temporalmente la revisión de los dispositivos ni fijó parámetros para ejecutarla, de modo que el amparado queda expuesto a una indagación sin delimitación alguna, que califican de “pesca por arrastre”, sin conocer la naturaleza ni el fundamento de las imputaciones.

Relatan que el 24 de agosto de 2026 pidieron audiencia de cautela de garantías para obtener acceso a las solicitudes de autorización de diligencias intrusivas citadas en la resolución de 19 de agosto y para que se regulara judicialmente la revisión de los dispositivos incautados, la extracción de la información pertinente y su incorporación a la carpeta fiscal. En la audiencia, celebrada el 26 de agosto de 2026, sostuvieron que el secreto del artículo 31 de la Ley N° 19.913 alcanza a la carpeta investigativa y no a la carpeta judicial electrónica, y pidieron que se circunscribiera el alcance de la revisión, excluyendo los antecedentes impertinentes, la información relativa a la vida privada de los intervinientes y las comunicaciones sostenidas con personas con derecho a guardar silencio, que se prohibiera la entrega de copias íntegras de los dispositivos y que se ordenara al Ministerio Público adoptar un protocolo de ejecución. El tribunal rechazó la primera petición, por estimar que los documentos pedidos, aunque integren la carpeta judicial, se refieren a antecedentes de la investigación sujetos a la reserva decretada conforme al citado artículo 31, y acogió parcialmente la segunda, sólo en cuanto limitó la revisión al período comprendido entre los años 2018 y 2026, declarando que “no cabe duda



que el persecutor tendrá acceso a información que será ciertamente impertinente y privada y no obstante, no es posible limitar esa posibilidad, porque de hacerlo se podría ver frustrada la investigación”.

En cuanto al derecho, sostienen, en primer término, que la negativa de acceso a la solicitud del Ministerio Público importa una aplicación analógica del artículo 31 de la Ley N° 19.913, proscrita por el inciso segundo del artículo 5° del Código Procesal Penal. Esa norma permite al fiscal disponer el secreto de la investigación, esto es, de los antecedentes de la carpeta investigativa en que se registra la actividad del persecutor y de las policías conforme al artículo 181 del mismo Código, mientras que el artículo 2° letra c) de la Ley N° 20.886 consagra la publicidad de la carpeta judicial electrónica, salvo las excepciones legales, entre las que el artículo 31 no se cuenta; extender el secreto a los antecedentes incorporados a la carpeta judicial por su sola vinculación con una investigación reservada supone trasladar la regla a un caso no comprendido en ella mediante un razonamiento de semejanza y no de subsunción, lo que la Corte Suprema ha vedado incluso respecto de leyes especiales que autoricen la restricción de derechos del imputado. Agregan que, mientras la defensa no conozca la solicitud, la resolución de 19 de agosto carece del fundamento que exigen los artículos 9° y 36 del Código Procesal Penal, pues se limita a aludir a antecedentes cuyo tenor no expresa, lo que la Corte Suprema ha estimado contrario al deber de fundamentación; que el control de una diligencia intrusiva autorizada sin conocimiento del afectado sólo puede ser posterior a su ejecución y exige conocer los hechos y antecedentes sometidos al juez, pues de otro modo la posibilidad de controvertirla es meramente formal, con infracción del artículo 19 N° 3 de la Constitución, del artículo 8.2 letra c) de la Convención Americana sobre Derechos Humanos y del artículo 14.3 letra b) del Pacto Internacional de Derechos Civiles y Políticos; y que la Corte Suprema, a propósito del secreto del artículo 38 de la Ley N° 20.000, ha resuelto que esa atribución no puede quedar al margen del control jurisdiccional y que corresponde al juez de garantía adoptar las medidas necesarias para dar a la defensa la información mínima que requiere el ejercicio de sus derechos, y ha acogido un amparo contra la negativa de acceso a la carpeta judicial electrónica fundada en el secreto de la carpeta



investigativa. Precisan que no pretenden conocer una diligencia pendiente, pues las autorizadas se ejecutaron el 20 de agosto de 2026.

En segundo término, afirman que la negativa a limitar la revisión infringe el artículo 218 del Código Procesal Penal, que sólo permite retener o incautar la correspondencia del imputado cuando por motivos fundados sea previsible su utilidad para la investigación, y el artículo 220, que excluye de la incautación las comunicaciones con las personas que pueden abstenerse de declarar por parentesco o por secreto profesional, límites que el tribunal descartó al declarar que no es posible acotar el acceso del persecutor; que no es previsible que las comunicaciones del amparado con su cónyuge y sus hijos, sus fotografías o los documentos relativos a su salud o a sus consultas legales sean útiles para la investigación; que la doctrina nacional advierte que una revisión carente de límites posibilita una búsqueda irrestricta en todo el acervo digital de la persona, contraria al principio de especialidad; y que la delimitación pedida es practicable y no obsta a la eficacia de la persecución, como lo muestran el protocolo que el Séptimo Juzgado de Garantía de Santiago fijó en marzo de 2025 para la revisión de los dispositivos incautados a una parlamentaria y el amparo que la Corte de Apelaciones de Valparaíso acogió en la causa Rol N° 3810-2026, que dispuso la custodia de los dispositivos por la Fiscalía, la individualización de los funcionarios con acceso a ellos, la delimitación temporal y material del análisis, la información de los parámetros de búsqueda y la eliminación de lo extraído fuera de esos límites. Concluyen que el acceso irrestricto autorizado constituye una injerencia ilegal en la vida privada y la correspondencia del amparado y de su familia, contraria a los numerales 4° y 5° del artículo 19 de la Constitución, al artículo 17 del Pacto y al artículo 11 de la Convención.

Piden que se acoja el amparo y se disponga que se permita a la defensa el acceso íntegro a la carpeta judicial electrónica de la causa, incluidos los antecedentes actualmente restringidos, y se le entregue copia de la solicitud del Ministerio Público que dio lugar a las diligencias intrusivas y de los demás antecedentes tenidos a la vista para resolverla; que la revisión y extracción de información de los dispositivos incautados el 20 de agosto de 2026 se sujete a un protocolo conforme al cual las especies permanezcan bajo custodia del Ministerio Público, con restricción del



acceso directo de las policías a la totalidad de su contenido, la búsqueda se limite a las comunicaciones y antecedentes relacionados con los hechos, personas y período objeto de la investigación, y se establezca un mecanismo que permita a la defensa conocer y controvertir la pertinencia de lo obtenido antes de su incorporación a la carpeta investigativa; y que se adopten las demás providencias necesarias para restablecer el imperio del derecho y asegurar la debida protección del amparado.

Segundo: Que las juezas del Cuarto Juzgado de Garantía de Santiago que dictaron las resoluciones impugnadas evacuaron los informes que les fueron requeridos. Daniela Verónica Guerrero González, jueza titular de ese tribunal, solicitó tener presente que, salvo mejor parecer de esta Corte, la resolución de 26 de agosto de 2026 no vulnera derecho constitucional alguno y fue dictada con estricta sujeción a la ley.

Expone que en la audiencia de 26 de agosto de 2026, celebrada para controlar las garantías de los imputados conforme al artículo 10 del Código Procesal Penal, las defensas de cuatro investigados, entre ellas la del amparado, pidieron copia de la solicitud que motivó la resolución de 18 de agosto de 2026 y que se regulara judicialmente el acceso del Ministerio Público y de las policías a los dispositivos electrónicos incautados, a lo que el persecutor se opuso, y que ninguna de esas alegaciones pretendía impugnar los fundamentos de la resolución que autorizó las medidas intrusivas. El tribunal rechazó la entrega de copias, por tratarse de antecedentes de la investigación sujetos a la reserva decretada por el Ministerio Público el 24 de julio de 2026 con arreglo al artículo 31 de la Ley N° 19.913, reserva que alcanza a toda la investigación aunque la solicitud sea anterior a la decisión del fiscal y aunque el imputado no esté directamente vinculado al delito de lavado de activos, y razonó que toda medida intrusiva afecta derechos y garantías, motivo por el cual exige autorización judicial previa, la que en este caso se dictó el 18 de agosto de 2026, y que la naturaleza de los delitos de corrupción explica que tales autorizaciones se otorguen sin conocimiento del afectado y en una investigación reservada.

Estimó que no es posible una exclusión *ex ante* de parte de la información, que la entrega de ésta no puede quedar al arbitrio de la persona investigada y que limitar el examen conforme a criterios previos



importaría una intromisión indebida en las facultades del persecutor y entorpecería el análisis, quedando a salvo la posibilidad de solicitar en su oportunidad la exclusión del medio probatorio. Reconoció, con todo, que el persecutor tendrá acceso a información impertinente y privada y que no es posible limitar esa posibilidad sin riesgo de frustrar la investigación.

En consecuencia, acogió la segunda solicitud sólo en cuanto la búsqueda de la información relativa a los hechos investigados deberá circunscribirse al período comprendido entre el año 2018 y el 20 de agosto de 2026, fecha de la incautación; prohibió la entrega a los intervinientes o a terceros, y la incorporación a la carpeta investigativa, de toda información contenida en los dispositivos ajena a los hechos; y ordenó al Ministerio Público sujetar su actuación a los instructivos contenidos en sus oficios 363/2025 y 983/2024, respecto de los cuales advirtió que dejan a salvo varias de las aprehensiones de los litigantes y que el tribunal no tenía inconveniente en que se plantearan complementaciones destinadas a limitar o aclarar el alcance de lo resuelto.

En cuanto al derecho, afirma que la resolución se ajusta a la normativa aplicable a los delitos económicos y a lo dispuesto en los artículos 218 y 220 del Código Procesal Penal. Sostiene que no extendió indebidamente el artículo 31 de la Ley N° 19.913, pues la incorporación de la solicitud de medidas intrusivas a la carpeta judicial, exigida por el artículo 9° del Código Procesal Penal para obtener la autorización, no muda su naturaleza de antecedente de la investigación, que es lo que la ley reserva, y que lo contrario permitiría que la sola exigencia legal de control jurisdiccional operase como una vía indirecta para sortear la reserva. Reconoce que toda medida intrusiva sobre un dispositivo de uso personal conlleva la posibilidad cierta de que el persecutor conozca información ajena a la investigación, circunstancia que tuvo presente al resolver, pero estima que ello no obliga a limitar el acceso *ex ante*, ya que el artículo 218 exige como resguardo la autorización judicial previa fundada en la utilidad de la diligencia, que fue observada, y el artículo 220 no opera como límite al acceso mismo sino como causal de exclusión probatoria, de modo que el amparado conserva el derecho a solicitar, en la oportunidad procesal correspondiente, la exclusión de las comunicaciones amparadas por los artículos 302 y 303 del mismo Código y a que la información impertinente no



sea considerada ni divulgada, siendo proporcionados y suficientes los resguardos adoptados respecto de sus comunicaciones familiares y de las sostenidas con personas obligadas al secreto profesional.

Francis Patricia Fell Franco, jueza titular del mismo tribunal, informó respecto de la resolución de 19 de agosto de 2026. Expone que la dictó a petición de la fiscal adjunta de la Fiscalía de Alta Complejidad, en una investigación por delitos previstos en la Ley N° 20.393, fraude al fisco, fraude informático, delitos contra la salud pública, falsificación de instrumento privado, cohecho y lavado de activos, y que se fundó en solicitudes previas del Ministerio Público, en medidas intrusivas autorizadas en julio de 2026 y en múltiples antecedentes, entre ellos informes de la Unidad de Análisis Financiero, documentación bancaria, transcripciones de audios, conversaciones de mensajería, comprobantes de transferencias y declaraciones, que dan cuenta de graves irregularidades de la empresa SOSER S.A. en la ejecución de contratos de alimentación escolar en la región de O'Higgins y, en lo que atañe al amparado, permiten presumir delitos de soborno y cohecho a funcionarios públicos para obtener información reservada y la adjudicación de licitaciones, en el marco de un mecanismo sostenido en el tiempo en el que participarían directivos de esa empresa, lobistas informales, funcionarios de la Junta Nacional de Auxilio Escolar y Becas y miembros del Congreso Nacional. Por ello estimó la diligencia necesaria, útil y proporcional conforme a los artículos 181, 187, 205, 209 y 217 del Código Procesal Penal, y autorizó por diez días la entrada y registro y la incautación de dispositivos y documentación en el domicilio particular y en el lugar de trabajo del amparado. Agrega que el 20 de agosto de 2026 la jueza Carolina Araya Hernández, a petición verbal de la fiscal, autorizó la entrada y registro de la oficina que el amparado ocupa en el edificio del ex Congreso Nacional, en calle Compañía de Jesús N° 1175, Santiago, para el solo efecto de cumplir la autorización del día anterior, y que la investigación se encuentra bajo la reserva decretada por el Ministerio Público el 24 de julio de 2026 conforme al artículo 31 de la Ley N° 19.913. Acompañó copia de la resolución de 19 de agosto y de la constancia de la autorización verbal, esta última suscrita con firma electrónica por la jueza que la otorgó.



Tercero: Que el Ministerio Público, por intermedio de la fiscal adjunta de la Fiscalía de Alta Complejidad y Crimen Organizado de la Fiscalía Regional Metropolitana Oriente a cargo de la investigación, acompañó, con ocasión de la vista de la causa, el Oficio FN N° 983/2024, de 16 de octubre de 2024, que imparte criterios de actuación en investigaciones penales complejas para el otorgamiento de copias, solicitud de diligencias y registro de información personal de interés investigativo, y el Oficio FN N° 363/2025, de 4 de abril de 2025, que lo complementa, a los que remite la resolución impugnada. De su contenido se dará cuenta más adelante. En estrados, el Ministerio Público no informó el estado en que se encuentra la extracción del contenido de los dispositivos incautados al amparado, si ella se completó o está pendiente, si se elabora un informe con su resultado ni la forma en que se conduce o conducirá la búsqueda de la información pertinente.

Cuarto: Que la acción constitucional de amparo, consagrada en el artículo 21 de la Constitución Política de la República, constituye un mecanismo de tutela de urgencia cuyo propósito es que la magistratura adopte de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado, frente a toda privación, perturbación o amenaza a su derecho a la libertad personal y seguridad individual que provenga de un acto u omisión contrarios a la Carta Fundamental o a las leyes.

Quinto: Que, como se advierte, el recurso impugna dos resoluciones dictadas por el Cuarto Juzgado de Garantía de Santiago en la causa RIT O-6719-2026. De la de 26 de agosto de 2026 cuestiona la negativa de acceso a la solicitud fiscal y a la carpeta judicial electrónica y, sobre todo, que permita al Ministerio Público y a las policías acceder al contenido íntegro de los dispositivos incautados al amparado sin un mecanismo de control o filtro previo, lo que, a su juicio, amenaza su libertad personal en relación con la vida privada y la inviolabilidad de las comunicaciones; de la de 19 de agosto reprocha la generalidad de su fundamentación y que no delimitara la revisión que autorizó. La recurrida no niega los hechos, sino que justifica su decisión en la ley y en los resguardos que adoptó, que estima suficientes. La cuestión principal a resolver consiste, entonces, en determinar si la jueza de garantía, al pronunciarse sobre la cautela pedida, satisfizo los deberes



que la Constitución y el Código Procesal Penal le imponen respecto de una diligencia que ella misma reconoció como lesiva de la privacidad del amparado y de terceros, o si, por el contrario, dejó la ejecución de esa diligencia sin el control que aquéllos exigen. De las restantes alegaciones se tratará una vez resuelta esa cuestión.

Sexto: Que, antes de entrar al fondo, conviene dejar sentado que la procedencia de esta acción ya fue resuelta. La Primera Sala de esta Corte la declaró inadmisibile el 3 de septiembre de 2026, por estimar que las alegaciones formuladas, cualquiera sea su mérito, no se enmarcan en las hipótesis que resguarda el artículo 21 de la Constitución; apelada esa resolución, la Corte Suprema la revocó el 17 de septiembre de 2026, en los autos Rol N° 50.141-2026, por considerar que la situación descrita en el recurso sí puede constituir uno de los supuestos previstos en ese precepto, y dispuso que una sala no inhabilitada diera al amparo la tramitación correspondiente “a fin de pronunciarse derechamente sobre el amparo deducido”.

Esa decisión se aviene con la doctrina que el máximo tribunal ha sostenido en casos semejantes, según la cual la libertad personal y la seguridad individual pueden verse amenazadas no sólo por vía principal, sino también de modo consecuencial, esto es, “con ocasión de la ejecución de un acto lesivo de uno o más derechos distintos”, y en ambos supuestos el amparo es el mecanismo idóneo para dejar sin efecto lo que ilegítimamente ponga en riesgo su ejercicio, pues reducir la acción a las afectaciones directas “importaría una injustificada restricción al derecho de accionar en procura de acceder a una tutela judicial efectiva” (SCS rol 12.292-2025, 28 de abril de 2025; en el mismo sentido, SCS rol 16.420-2025, 22 de mayo de 2025).

Por consiguiente, no corresponde a esta Sala volver sobre la admisibilidad y debe pronunciarse derechamente sobre la infracción denunciada.

Séptimo: Que los hechos relevantes no están discutidos. El 19 de agosto de 2026, en la investigación reservada que se sigue por delitos previstos en la Ley N° 20.393, fraude al fisco, fraude informático, delitos contra la salud pública, falsificación de instrumento privado, cohecho y lavado de activos, la jueza Francis Fell Franco, del Cuarto Juzgado de



Garantía de Santiago, autorizó por diez días la entrada y registro de diversos domicilios, entre ellos el domicilio particular del amparado en Coquimbo y su lugar de trabajo en el Congreso Nacional, y la incautación de teléfonos celulares, computadores y demás dispositivos de almacenamiento digital de titularidad de las personas que individualizó, entre ellas el amparado, “que pudieran dar cuenta de reuniones, intercambios de información y otras formas de comunicación relacionadas a los hechos investigados”, así como la incautación y el acceso a sus cuentas de correo electrónico institucionales del Senado y del Congreso Nacional, y autorizó al persecutor y a la policía “el acceso, revisión, extracción y análisis de la información contenida en los dispositivos electrónicos incautados”, comprensiva de sus memorias internas y externas, de la tarjeta SIM, de las imágenes, videos, audios y de todo dato y registro almacenado en ellos, “así como en sus aplicaciones, redes sociales, correos electrónicos y nubes de almacenamiento a las que se halle vinculado el dispositivo”, sin acotar el período ni las materias de interés. Es la resolución a la que el informe de la jueza recurrida y la resolución impugnada se refieren como de 18 de agosto. El 20 de agosto, la jueza Carolina Araya Hernández, del mismo tribunal, autorizó, a petición verbal de la fiscal y para el solo efecto de cumplir esa resolución, la entrada y registro de la oficina del amparado en el edificio del ex Congreso Nacional, en Santiago, según la constancia suscrita con firma electrónica que se acompañó al informe; ese mismo día la Policía de Investigaciones practicó la diligencia e incautó los dispositivos del amparado, y el 24 de agosto su defensa pidió la cautela de sus garantías. El 26 de agosto la jueza recurrida, al resolverla, negó el acceso a la solicitud fiscal, acotó temporalmente la búsqueda, prohibió entregar e incorporar a la carpeta lo ajeno a los hechos y remitió a dos instructivos internos del Ministerio Público, pero declinó fijar cualquier otro límite a la ejecución de la extracción, con la advertencia de que el persecutor accederá a información impertinente y privada. Lo que se examina en primer lugar, por ende, no es la legalidad de la incautación ni la de la autorización para revisar los dispositivos, cuyos presupuestos el recurso no discute, pues su reproche a la resolución de 19 de agosto, del que se tratará más adelante, se dirige a la generalidad con que expresa sus fundamentos y a la falta de límites de la



revisión, sino la suficiencia de los términos en que el tribunal dejó que esa revisión se ejecute.

Octavo: Que la respuesta exige partir de lo que hoy es un teléfono inteligente. Ningún otro objeto concentra tanta información sobre una persona. Acompaña a su dueño a toda hora; por él transitan sus conversaciones, sus fotografías, sus pagos y sus cuentas bancarias, su trabajo y la administración de su casa, y en su memoria se superponen, sin separación posible, la vida laboral, la doméstica y la afectiva. Tampoco admite, a diferencia del domicilio, un acotamiento espacial, pues en una casa puede registrarse una habitación y dejar cerradas las demás, mientras que quien accede a un teléfono accede a todo lo que contiene. La Corte Suprema de los Estados Unidos lo describió en *Riley v. California*. Estos aparatos, dijo, son en realidad minicomputadores que reúnen en un solo lugar distintas clases de información, cuya combinación revela mucho más que cualquiera de ellas por separado; la suma de la vida privada de una persona puede reconstruirse a partir de un millar de fotografías fechadas y localizadas; la mayoría de sus dueños lleva consigo “un registro digital de casi todos los aspectos de sus vidas”; y un registro del teléfono “expondría típicamente al gobierno mucho más que el registro más exhaustivo de una casa” (*Riley v. California*, 573 U.S. 373, 393-397 y 403, 2014).

La misma idea llevó al Tribunal Constitucional Federal alemán a reconocer un derecho fundamental autónomo a la confidencialidad e integridad de los sistemas informáticos, comprensivo de los teléfonos móviles con múltiples funciones, al constatar que el acceso estatal a sistemas que contienen datos personales en tal cantidad y variedad permite reconstruir aspectos esenciales de la vida de una persona e incluso elaborar un perfil completo de su personalidad, y que ese riesgo existe ya en medidas de acceso aislado, como la incautación o copia de los soportes de almacenamiento, cuyos registros pueden incluir la correspondencia privada y profesional y anotaciones de carácter íntimo (BVerfG, sentencia de 27 de febrero de 2008, 1 BvR 370/07 y 1 BvR 595/07, BVerfGE 120, 274). El mismo tribunal advirtió que la gravedad de la injerencia aumenta cuando los datos revelan las comunicaciones del afectado con terceros, ya que la medida alcanza indiscriminadamente a esos interlocutores, respecto de los cuales no concurren los presupuestos que la justifican (*ibídem*).



Lo dicho vale, con igual o mayor razón, para los computadores y demás dispositivos de almacenamiento masivo de información, que contienen datos de la misma naturaleza y se examinan del mismo modo, de manera que los razonamientos de esta sentencia les son aplicables con las adaptaciones que su distinta configuración exija. Si el análisis se centra en el teléfono es porque en él concurren con mayor intensidad las características descritas, sin perjuicio de que, según el recurso, al amparado se le incautó también su computador y de que la resolución de 19 de agosto de 2026 autorizó la incautación de computadores, discos duros y otros soportes.

Noveno: Que a esa constatación se suma la forma en que la diligencia se ejecuta. La revisión de un teléfono incautado no consiste en abrir una carpeta determinada, sino en obtener, mediante herramientas forenses, una copia íntegra de su contenido, la llamada copia espejo, sobre la cual se practica después la búsqueda de lo pertinente. Al extraer, la técnica no distingue lo útil de lo que no lo es; se copia todo, desde los registros de las aplicaciones de mensajería y de correo hasta las fotografías, incluida la información personal, íntima y familiar del titular, y sólo con posterioridad se determina qué sirve a la investigación. Desde el punto de vista jurídico, generar esa copia equivale a apoderarse de todos los datos aunque el aparato se devuelva, porque el funcionario que la obtiene no sabe qué contenido ha copiado, sino sólo que ha tomado una copia de cuanto había en el dispositivo (Kerr, O. S., “Fourth Amendment Seizures of Computer Data”, en Yale Law Journal, vol. 119, 2010, pp. 709 y 717).

Por eso la lesión no se atenúa por la circunstancia de que el persecutor, una vez en posesión del acervo completo, seleccione después lo que quiere examinar, que es el supuesto del que parte la resolución recurrida cuando remite la protección a la exclusión probatoria posterior. La injerencia se consuma con la copia, no con el uso; desde ese momento el Estado dispone de toda la información y el afectado depende de la buena disposición del órgano que la tiene. La Corte Suprema estadounidense lo advirtió recientemente a propósito de los registros de localización que un servicio conserva de sus usuarios, al sostener que el alcance de la invasión “no se hace menor porque el gobierno, con el beneficio de la retrospectiva,



pueda señalar exactamente qué pocas horas de desplazamientos quiere revisar” (Chatrie v. United States, No. 25-112, sentencia de 29 de junio de 2026, slip op. p. 21). En términos análogos, el Tribunal Europeo de Derechos Humanos ha subrayado que la separación de lo protegido y lo que no lo está adquiere especial relevancia cuando la incautación recae sobre grandes volúmenes de datos digitales o se practica mediante una copia espejo, y que resulta esencial impedir todo acceso no autorizado ni registrado a esos datos desde su incautación hasta su devolución o destrucción (TEDH, Särgava c. Estonia, N° 698/19, 16 de noviembre de 2021). De ahí que el control no pueda diferirse al momento en que el persecutor decida usar la información, sino que deba recaer sobre la conservación misma de la copia, que es donde reside la afectación.

En el caso, la resolución recurrida da cuenta de esa realidad. La jueza dejó constancia de que “no es posible una exclusión ex ante de parte de la información contenida en los dispositivos” y de que “no cabe duda de que el persecutor tendrá acceso a información que será impertinente y privada”. La afectación que aquí se examina no es, entonces, hipotética ni discutida; está reconocida en el acto impugnado y se extiende a terceros que no son imputados, como los familiares cuyas fotografías y mensajes alberga el aparato o las personas que se comunicaron con el amparado, cuya privacidad quedará expuesta sin que a su respecto concorra sospecha alguna.

A ello se agregan dos circunstancias propias de este caso. La primera es que, según expone el recurso, los dispositivos contienen las comunicaciones del amparado con su cónyuge y sus hijos, información relativa a su salud y sus consultas con abogados. Esa información pertenece en parte a esos terceros y toca en todo caso el núcleo de la vida privada del amparado; y sus comunicaciones con quienes asumen su defensa están, además, cubiertas por el derecho que los artículos 8.2 letra d) de la Convención Americana sobre Derechos Humanos y 14.3 letra b) del Pacto Internacional de Derechos Civiles y Políticos aseguran a todo inculpado de comunicarse libre y privadamente con su defensor, y por el secreto que el artículo 303 del Código Procesal Penal reconoce al abogado en beneficio de su cliente. Se trata, pues, de información que, en cuanto ajena a los hechos investigados, ni el persecutor ni terceros debieran llegar



a conocer, y que por lo mismo debe quedar excluida de la búsqueda y eliminada de la copia obtenida o que se esté obteniendo, como se dispondrá. El Tribunal Europeo de Derechos Humanos ha exigido garantías procedimentales específicas cuando el material incautado o copiado contiene comunicaciones entre abogado y cliente, incluso cuando el sospechoso es el propio abogado, porque lo protegido es la confianza del cliente y la posición que la abogacía ocupa en la administración de justicia, y ha reprochado que la orden de registro se limite a señalar que los investigadores accederán sólo a los datos relevantes, sin prever resguardo concreto alguno para el material amparado por el secreto (Särgava c. Estonia; Nezirić c. Bosnia y Herzegovina).

La segunda es que, hasta ahora, ninguna otra limitación se ha fijado. Como se dejó constancia, en estrados el Ministerio Público no informó el estado de la extracción, si ésta se completó o está pendiente, si se elabora un informe con su resultado ni cómo se conduce la búsqueda dentro de la copia; y la resolución de 19 de agosto de 2026 autorizó el acceso a todo el contenido de los dispositivos y de los servicios vinculados a ellos, y a las cuentas de correo institucionales del amparado, sin acotar materias, personas ni período. El único patrón que hoy delimita el examen es el temporal que la jueza recurrida impuso el 26 de agosto. Todo lo demás, esto es, qué se busca, con qué criterios, quiénes acceden y qué ocurre con lo que no interesa, queda librado al arbitrio del órgano que ejecuta la diligencia.

Décimo: Que la intromisión no se agota en la memoria del aparato. El teléfono es, además, la llave de acceso a los servicios en línea que su titular mantiene con la cuenta abierta, esto es, cuentas de correo, redes sociales de acceso restringido, mensajería sincronizada y repositorios de almacenamiento en la nube, cuya información no está necesariamente grabada en el dispositivo, sino en servidores externos, con frecuencia situados fuera del país, pero a la que se accede directamente desde el aparato con sólo pulsar la pantalla. Quien examina un teléfono desbloqueado puede alcanzar por esa vía información que nunca estuvo en poder de la policía, que el titular considera suya aunque la custodie un tercero y que en muchos casos pertenece también a otras personas, como ocurre con los grupos de mensajería, los perfiles cerrados de una red social



o las carpetas compartidas. La Corte Suprema de los Estados Unidos advirtió en Riley que los datos que el usuario ve en su teléfono pueden no estar almacenados en él, que los agentes que revisan el aparato no sabrán normalmente si lo que miran estaba en el dispositivo o proviene de la nube, y que extender a esos archivos el registro del teléfono sería como encontrar una llave en el bolsillo de un sospechoso y sostener que ella autoriza a abrir y registrar una casa (Riley v. California, 573 U.S. 373, 397-398); y en Chatrie agregó que los registros que un servicio guarda en sus servidores se asemejan a los correos, documentos, fotografías o calendarios que el usuario razonablemente considera propios aunque estén alojados en servidores ajenos (Chatrie v. United States, slip op. p. 18). El Tribunal Constitucional Federal alemán, por su parte, incluyó expresamente en el ámbito del derecho a la confidencialidad e integridad de los sistemas informáticos los datos a los que el sistema da acceso en virtud de sus conexiones de red (BVerfG, sentencia de 27 de febrero de 2008).

Entre nosotros ese salto no es de cantidad sino de naturaleza. El acceso remoto a un dispositivo, computador o sistema informático mediante programas computacionales, contraseñas, códigos de seguridad o de acceso es una diligencia distinta, que el artículo 225 bis del Código Procesal Penal somete a petición fundada del Ministerio Público, a la existencia de fundadas sospechas basadas en hechos determinados y a una autorización judicial específica, sujeta a un plazo máximo y a los requisitos de contenido que detalla el artículo 225 ter. Servirse de la sesión abierta en el teléfono incautado para ingresar a esos repositorios produce el mismo efecto que el registro remoto, con la diferencia de que se obtiene sin la resolución fundada que la ley exige para él; por eso no puede entenderse comprendido en la autorización para revisar el contenido del aparato y requiere una autorización expresa, que precise el servicio, la cuenta y el alcance del acceso. Así lo dispone, para el registro remoto, el artículo 225 quáter del mismo Código, que exige, a petición fundada del Ministerio Público, una nueva autorización del juez de garantía con las especificaciones del artículo 225 ter cuando al ejecutarlo surjan motivos para creer que los contenidos buscados están almacenados en otro sistema informático. La Ley de Enjuiciamiento Criminal española lo resuelve en términos semejantes, al exigir autorización judicial para ampliar el registro desde el dispositivo



incautado a los datos almacenados en otro sistema informático accesible desde él, salvo que la autorización inicial ya la comprenda, según su artículo 588 sexies c, apartado 3. En este caso, la resolución de 19 de agosto de 2026 extendió la autorización, en términos genéricos, a las aplicaciones, redes sociales, correos electrónicos y nubes de almacenamiento a las que se halle vinculado el dispositivo, sin individualizar servicios ni cuentas, sin acotar el período y sin las especificaciones que el artículo 225 ter exige para el registro remoto. Esa autorización es objetada por el recurso por su falta de límites, y su ejecución queda comprendida en el problema que aquí se resuelve, pues el acceso a esos repositorios multiplica el volumen de información privada, del amparado y de terceros, que el persecutor obtendrá. De ahí que las medidas de control que se dispondrán deban alcanzarlo, y que el Ministerio Público deba informar al tribunal a qué servicios y cuentas ha accedido o accederá por esa vía, para que el juez de garantía delimite ese acceso con arreglo a los artículos 225 bis, 225 ter y 225 quáter.

Undécimo: Que la lesión así descrita no proviene de la ley, que nada dice sobre la revisión del teléfono incautado, sino de la resolución judicial que autoriza la diligencia y fija, o deja de fijar, sus términos. El artículo 9° del Código Procesal Penal somete a autorización judicial previa toda actuación del procedimiento que prive al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o los restrinja o perturbe, y el inciso segundo del artículo 5° ordena interpretar restrictivamente las disposiciones que autorizan la restricción de la libertad o de otros derechos del imputado. Si la ley confía al juez esa autorización, es porque espera de él algo más que un permiso; espera que pondere la intensidad de la injerencia frente al interés de la persecución y que la limite a lo que ese interés requiere. El principio de proporcionalidad, con sus exigencias de idoneidad, necesidad y proporcionalidad en sentido estricto, es el método con que esa ponderación se realiza, y la doctrina nacional ha sostenido que el juez de garantía debe practicar ese test antes de decretar cualquier medida restrictiva de derechos fundamentales, comprobando que la diligencia sea adecuada al fin que se pretende, eligiendo entre las medidas idóneas la menos lesiva y verificando que las ventajas de la autorización guarden correspondencia con la vulneración que causa (Núñez Ojeda, R., Beltrán Calfurrapa, R. y Santander



Akklass, N., “Los hallazgos casuales en las diligencias de incautación e intervención de las comunicaciones digitales en Chile. Algunos problemas”, en *Política Criminal*, vol. 14, N° 28, 2019, pp. 159-160 y 180).

La Corte Suprema ha situado esa exigencia en el centro del control de las diligencias intrusivas, al declarar que el tribunal está obligado a requerir del persecutor las precisiones necesarias para despejar cualquier situación incierta, “principalmente para satisfacer correctamente el estándar de proporcionalidad que conlleva acceder a una diligencia invasiva de derechos fundamentales” (SCS rol 12.292-2025, 28 de abril de 2025). Trasladado ese estándar a la revisión de un teléfono, el juicio de necesidad impone al juez adoptar las medidas que reduzcan la afectación de la privacidad al mínimo compatible con el éxito de la investigación, y ello con mayor razón cuando la injerencia alcanza a terceros ajenos al proceso, que no han sido oídos ni pueden defenderse. Una autorización que reconoce que el persecutor accederá a información impertinente y privada y, en el mismo acto, renuncia a fijar cómo se acotará ese acceso y qué ocurrirá con lo excedente, no supera ese juicio.

Duodécimo: Que la intensidad de esta injerencia es, cuando menos, equivalente a la de las medidas que el Código sí regula con detalle. La interceptación de comunicaciones capta lo que se dice mientras se dice; el registro remoto de equipos informáticos aprehende el contenido de un sistema sin conocimiento del usuario; la extracción del teléfono incautado toma de una vez todo lo que se dijo, se escribió, se fotografió y se guardó durante años. Para las dos primeras el legislador exige fundadas sospechas basadas en hechos determinados. Sujeta la interceptación a delitos con pena de crimen y a que la investigación la haga imprescindible, y ordena que la resolución individualice al afectado, singularice los medios a intervenir y señale al funcionario encargado, la forma, el alcance y la duración de la medida, que no puede exceder de sesenta días prorrogables sólo previo examen de la subsistencia de sus requisitos, como dispone el artículo 222; y limita el registro remoto a un plazo máximo de treinta días, prorrogable bajo la misma condición, conforme al artículo 225 bis. El artículo 225 ter, a su vez, exige que la resolución que autoriza el acceso remoto especifique los dispositivos objeto de la medida, “el alcance de la medida, la forma en la que se procederá al acceso y aprehensión de contenidos



relevantes para la causa”, los agentes autorizados, la autorización para realizar y conservar copias, las medidas técnicas de preservación y “la duración precisa de la medida”. Y, cumplida la interceptación, el inciso cuarto del artículo 223 manda entregar a los afectados las comunicaciones impertinentes o irrelevantes y ordena que el Ministerio Público destruya toda transcripción o copia de ellas.

La Corte Suprema ha recordado que, por ser excepcionales las medidas que afectan la intimidad, la vida privada y la inviolabilidad de las comunicaciones, “el legislador exige un alto estándar de exigencias que deben cumplirse tanto por la fiscalía -para solicitarlas- como de motivación por el juez al dictar la resolución que las dispone” (SCS rol 18.430-2025, 3 de junio de 2025). No sería coherente que la diligencia más invasiva de todas, la que abarca a la vez las comunicaciones pasadas, las imágenes, los documentos, los desplazamientos y las relaciones del titular con terceros, quedara sometida a exigencias menores que la interceptación o el registro remoto por el solo hecho de que el Código, promulgado en el año 2000, cuando los teléfonos móviles no tenían las capacidades actuales, no la menciona, silencio que las reformas posteriores no han llenado, ni siquiera la Ley N° 21.577, que reguló el registro remoto de equipos informáticos, a diferencia de lo ocurrido en España, donde desde 2015 la ley disciplina de modo específico el registro de los dispositivos de almacenamiento masivo de información. El principio de proporcionalidad conduce a lo contrario, pues obliga a exigir de la petición del persecutor y de la resolución que la acoge, al menos, el mismo nivel de fundamentación y de precisión que el legislador impone a aquéllas.

Ninguna objeción cabe oponer a que esas exigencias se extiendan por vía analógica a una diligencia que la ley no regula. La prohibición de analogía del inciso segundo del artículo 5° del Código Procesal Penal alcanza a las disposiciones que autorizan la restricción de la libertad o de otros derechos del imputado, no a las que la condicionan o limitan; trasladar a la revisión del teléfono incautado los resguardos previstos para el registro remoto opera en beneficio del afectado y responde al deber que el inciso segundo del artículo 5° de la Constitución impone a los órganos del Estado de respetar y promover los derechos esenciales que emanan de la naturaleza humana. Por lo demás, si el acceso clandestino a un sistema



informático debe acotarse en su alcance, forma, agentes, copias y duración, no se advierte por qué habría de quedar exento de esos límites el acceso que, sin ser clandestino, es compulsivo e impuesto, pues en uno y otro caso falta la voluntad del usuario para el registro y revisión de sus datos, y ante un grado equivalente de afectación de la garantía corresponden resguardos equivalentes.

El derecho comparado confirma esta orientación. La Ley de Enjuiciamiento Criminal española somete las medidas de investigación tecnológica a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, declara que “la simple incautación” de un teléfono u otro dispositivo de almacenamiento masivo “no legitima el acceso a su contenido”, exige una motivación individualizada para autorizarlo y dispone que la resolución que lo permite “fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos”, según sus artículos 588 bis a) y 588 sexies a), b) y c). Allí donde el legislador ha regulado la materia, en suma, no ha admitido que el acceso al contenido de un teléfono siga automáticamente a su incautación ni que la orden pueda omitir el alcance del registro y el destino de las copias.

Décimo tercero: Que de lo anterior se sigue el contenido mínimo que debe tener la resolución que autoriza la extracción y revisión de un teléfono. No basta con permitir el “peritaje” o el “vaciado” del aparato, porque sin determinación del objeto no hay modo de saber después qué fue búsqueda y qué fue hallazgo. El artículo 36 del Código Procesal Penal obliga a expresar “sucintamente, pero con precisión, los motivos de hecho y de derecho” de la decisión, y la Corte Suprema ha declarado que ese mandato integra las garantías mínimas del debido proceso y no se satisface con la mera relación de los antecedentes o de las solicitudes de los intervinientes (SCS rol 14.900-2024, 9 de mayo de 2024; SCS rol 12.292-2025, 28 de abril de 2025). Aplicado a esta diligencia, el deber de fundamentación exige que el juez requiera del Ministerio Público, y consigne en su resolución, cuál es la información que se busca, determinada por los hechos investigados, las personas o cuentas con las que se pretende establecer comunicación, la época a que se refiere y las categorías de contenido pertinentes, así como la manera en que, obtenida la copia íntegra, se identificará lo útil y el plazo dentro del cual lo restante será eliminado de esa copia. Si el persecutor



sostiene que alguna de esas determinaciones es técnicamente imposible, a él corresponde justificarlo ante el juez, y no al afectado demostrar lo contrario.

La proposición de esos criterios corresponde al Ministerio Público y no al juez. Definir los descriptores de una búsqueda dirigida, sean palabras clave, interlocutores, cuentas, tipos de archivo o rangos de fechas, es una función investigativa que exige el dominio de los antecedentes reunidos, de la hipótesis que se indaga y de las técnicas forenses e informáticas con que se examina una copia, conocimientos que el tribunal no posee y que el artículo 83 de la Constitución radica en el persecutor. Lo que el juez puede y debe exigir es que esa propuesta exista antes de que la copia se examine, que quede registrada, que sea puesta en su conocimiento y que sea razonable, pues sólo así el control posterior contará con un punto de referencia contra el cual medir lo que se hizo. Este último requisito no es menor. Unos criterios tan amplios que capturen la mayor parte del contenido, como sería buscar por términos de uso corriente o por interlocutores indeterminados, equivalen a no tener criterios, y bajo su apariencia la revisión termina por abarcarlo todo, de modo que cuanto aparezca podrá presentarse después como un hallazgo casual que en realidad estaba preconstituido por la amplitud de la búsqueda; frente a una propuesta de esa índole, el juez debe exigir su acotamiento antes de que el examen comience. Así lo entendió la Corte de Apelaciones de Valparaíso en un amparo reciente, deducido por una imputada contra la negativa del juez de garantía a limitar el examen de los dispositivos que le fueron incautados, al ordenar que los descriptores de búsqueda fueran informados al juzgado de garantía (SCA de Valparaíso rol 3810-2026, 1 de septiembre de 2026, confirmada por SCS rol 49.866-2026, 24 de septiembre de 2026, con declaración sobre las medidas a cargo del Ministerio Público).

Esos criterios han de aplicarse, ante todo, a las aplicaciones de mensajería, al correo electrónico y a las redes sociales, que son hoy el principal depósito de las comunicaciones de una persona y, previsiblemente, el objeto central del examen, y no sólo a los archivos que el aparato guarda en sus carpetas. Sus registros forman parte del contenido extraído, sea que estén almacenados en el dispositivo o que la aplicación los sincronice desde servidores externos a través de la cuenta abierta,



según se dijo en el considerando décimo, y quedan sujetos a las mismas limitaciones. Respecto de ellos, la delimitación por cuenta, interlocutor y período es la que permite que el persecutor lea las conversaciones y los correos intercambiados con las personas y en la época que interesan a la investigación, y no la totalidad de los intercambios del amparado con quienes nada tienen que ver con ella, mientras que las palabras clave y las categorías de contenido cumplen esa función respecto de las conversaciones de grupo y de las casillas con numerosos remitentes. Las herramientas de análisis forense permiten filtrar los registros extraídos por contacto, cuenta, fecha y término de búsqueda, de modo que la limitación no es impracticable y, si el persecutor sostuviere lo contrario en algún caso, deberá justificarlo ante el juez.

Distinto es el caso de las fotografías, los videos y los audios. Su contenido no está expresado en texto, de modo que las palabras clave no permiten seleccionarlos; lo que sí permite acotar el universo son los datos asociados a cada archivo, esto es, la fecha en que se creó o recibió, el lugar en que se captó y la conversación, correo o cuenta de la que proviene. Por eso, respecto de estos archivos, la limitación opera a través del período y de la procedencia, y dentro del conjunto así delimitado no hay otro modo de saber si son pertinentes que verlos u oírlos, revisión directa que, por lo mismo, importa una intromisión mayor y exige, como compensación, que la practiquen sólo los funcionarios individualizados, que no se generen copias adicionales, que se deje constancia de los archivos que se conservan y que los restantes, entre ellos los de carácter personal y familiar, cuya revisión íntegra objeta el recurso, se eliminen con el excedente. Pretender que el persecutor identifique lo útil sin mirar sería tan ilusorio como permitirle mirar sin límite y sin registro.

La experiencia europea muestra el costo de omitir esas determinaciones. En *Särgava c. Estonia*, el Tribunal Europeo de Derechos Humanos constató que la orden de registro no previó resguardo alguno para el material protegido, que la búsqueda por palabras clave sobre la copia del teléfono y del computador de un abogado no derivaba de la ley ni de la orden, sino de una decisión de los propios investigadores, quienes eligieron términos tan amplios como “ejercicio financiero” o “línea de crédito”, y que el derecho interno no ofrecía mecanismo alguno para que el material



disputado no llegara a los investigadores antes de que un tribunal lo analizara y, de ser necesario, ordenara su devolución o destrucción; por ello declaró violado el artículo 8 del Convenio. Y en *Nezirić c. Bosnia y Herzegovina* reiteró que copiar íntegramente el teléfono de un abogado y filtrar la copia con los números de los coimputados, sin que esa limitación proviniera de la ley ni estuviera sujeta a supervisión judicial, carece de las garantías procedimentales que exige el Convenio (TEDH, *Nezirić c. Bosnia y Herzegovina*, N° 4088/21, 5 de noviembre de 2024).

Décimo cuarto: Que, si el persecutor no ofrece esa delimitación, el juez debe exigirla y, en su defecto, establecerla. La cautela de garantías del artículo 10 del Código Procesal Penal lo faculta para adoptar, “de oficio o a petición de parte, las medidas necesarias” para permitir el ejercicio de los derechos del imputado, y el artículo 14 letra a) del Código Orgánico de Tribunales le encomienda “asegurar los derechos del imputado y demás intervinientes en el proceso penal”. En una diligencia que necesariamente pasa por la copia total del dispositivo, esas medidas consisten, cuando menos, en fijar un plazo para culminar la extracción y la identificación del contenido útil, en ordenar la eliminación del resto de la copia con certificación de haberse practicado y en resolver sobre la devolución del aparato o, si su conservación es necesaria, sobre su custodia. Nada de ello es ajeno a nuestro sistema. El deber de destruir las copias de lo impertinente ya está en el inciso cuarto del artículo 223 para las interceptaciones, y no se advierte razón para excluir de él a un registro que compromete la privacidad con mayor intensidad; la fijación de plazos y de una duración precisa está en los artículos 222 y 225 ter; y la custodia de lo incautado, con acceso de los intervinientes autorizado por el fiscal o, en su caso, por el juez de garantía, en el artículo 188.

El Tribunal Constitucional Federal alemán llegó a la misma solución cuando admitió que, en el acceso a sistemas informáticos, es prácticamente inevitable obtener información antes de poder determinar si pertenece al núcleo de la vida privada; en tal caso, dijo, la protección debe asegurarse en la fase de análisis, mediante un procedimiento que examine los datos recogidos y disponga que los que pertenezcan a ese núcleo se eliminen sin dilación y no puedan utilizarse ni transmitirse (BVerfG, sentencia de 27 de febrero de 2008). En el ámbito del Convenio Europeo, el control judicial



posterior fue la garantía decisiva en *Sérvulo & Asociados c. Portugal*, donde no se declaró violación porque el juez de instrucción revisó lo incautado en un estudio de abogados y ordenó destruir cerca de 850 archivos que contenían información personal, cubierta por el secreto profesional o relativa a personas no investigadas (TEDH, *Sérvulo & Asociados - Sociedade de Advogados, RL y otros c. Portugal*, N° 27013/10, 3 de septiembre de 2015). Y entre nosotros, el fallo de la Corte de Apelaciones de Valparaíso ya citado dispuso, además de la comunicación de los descriptores de búsqueda, que el Ministerio Público informara al tribunal los funcionarios con acceso a los dispositivos, dejara fuera del análisis lo impertinente y eliminara toda la información extraída fuera de esos límites, informando los protocolos seguidos y las personas encargadas. Al confirmarlo, la Corte Suprema declaró que los dispositivos incautados y su custodia deben quedar únicamente a cargo del fiscal responsable de la investigación, que el Ministerio Público debe informar al juez de garantía el nombre de los funcionarios que tendrán acceso a ellos, que no puede utilizarse información anterior a la época que fijó, que debe quedar fuera de análisis toda la información que carezca de pertinencia con los hechos que justificaron la incautación, a excepción de los hallazgos que puedan revestir caracteres de otros ilícitos, y que toda la información extraída fuera de esos límites, y de la que se hubieren hecho copias sin interés criminalístico, debe ser eliminada, informando al tribunal los protocolos seguidos y las personas encargadas de su ejecución. Recordó, asimismo, que el Código no sólo regula los casos y formas de la interceptación, sino también, en el artículo 223, el destino de la información obtenida, como lo hace el inciso final del artículo 218 para la correspondencia.

Décimo quinto: Que la determinación del objeto tiene otra consecuencia, referida a los hallazgos que se produzcan durante la revisión. El artículo 215 del Código Procesal Penal permite incautar los objetos o documentos que, durante la práctica de un registro, hagan sospechar la existencia de un hecho punible distinto. Esa regla se concibió para la entrada y registro en lugares cerrados, donde las divisiones físicas permiten deslindar lo autorizado de lo que no lo está. En el interior de un teléfono no hay habitaciones ni cajones que separen unos contenidos de otros; todo



está al alcance del mismo examen. Si bastara, entonces, con que un contenido apareciera durante la revisión para autorizar su uso, la orden que recae sobre un teléfono se convertiría en una orden sobre todo el teléfono, y la determinación de su objeto perdería todo sentido. La doctrina ha advertido que, conforme al principio de especialidad, no es admisible una incautación destinada a descubrir, sin la adecuada precisión, actos delictivos cualesquiera, lo que convertiría la orden en una autorización en blanco, y que admitir el hallazgo casual sin límites llevaría a que “cualquier incautación de un dispositivo informático se transforme en una búsqueda general, habilitada para capturar cualquier evidencia de cualquier delito” (Núñez Ojeda, R., Beltrán Calfurrapa, R. y Santander Akkrass, N., *ob. cit.*, pp. 173 y 180; en el mismo sentido, pp. 176-177).

De ahí que el persecutor no pueda servirse de la copia para revisar el teléfono en busca de otros delitos. Si la orden no fija límites a la revisión, todo lo que aparezca en la copia será, por definición, encontrado “casualmente”, y la excepción del hallazgo casual, pensada para lo que surge sin buscarlo, terminará por cubrir lo que la orden debía impedir, esto es, la revisión exploratoria de todo el contenido en busca de algún delito, sin saber cuál, que la doctrina y la jurisprudencia comparadas llaman investigación prospectiva. Con límites, en cambio, el hallazgo es casual sólo cuando se produce de manera inevitable en el curso de la ejecución legítima de la orden y dentro de ellos; cuando la revisión se extiende deliberadamente a contenidos que la orden no cubría, lo encontrado no es fruto del azar, sino de una desviación de la orden judicial que no puede aprovecharse. Es al Ministerio Público a quien corresponde acreditar que la ejecución de la orden, respetado el principio de especialidad, conducía necesariamente a la información del delito distinto, porque es él quien conduce el examen, quien está en condiciones de registrar cómo se practicó y sobre quien pesa el deber de fundamentar sus actuaciones. Esta Corte ya advirtió, al conocer de una acción de protección referida a la transcripción de centenares de miles de páginas de mensajería extraídas de un teléfono, que la orden judicial sólo pudo referirse a las conversaciones relacionadas con el objeto de la investigación y que es deber del Ministerio Público cautelar, en su labor, los derechos constitucionales de los terceros ajenos a ella (SCA de Santiago rol 6423-2024, 28 de junio de 2024); y el voto de



minoría de ese fallo, que estuvo por acoger la acción, precisó que el persecutor no puede, sin incurrir en ilegalidad, hurgar en esas transcripciones en una suerte de búsqueda de ilícitos ajenos al objetivo de la orden judicial, pues el orden correcto es el inverso, esto es, iniciar una investigación por un delito determinado y, según los datos que ella arroje, solicitar la autorización para develar los mensajes, sin que la autorización otorgada constituya “una especie de patente de corso” para buscar y rebuscar en ellas algún ilícito distinto del que inició la investigación. Cuando, en el curso de la revisión legítima, aparezca información sobre otro hecho punible, lo procedente será ponerla en conocimiento del juez de garantía y obtener de él la autorización para utilizarla, con el umbral de gravedad que el inciso final del artículo 223 fija para la información obtenida en una interceptación, analogía que se impone por la equivalente intensidad de ambas injerencias, en lugar de acudir a la más laxa del artículo 215, pensada para un continente físico.

Ese control se ejerce después de la revisión y tiene un objeto preciso. Corresponde al juez que autorizó la diligencia, aunque la investigación del nuevo delito llegue a radicarse ante otro tribunal, porque es él quien fijó los límites de la orden y recibió los criterios de búsqueda, de modo que sólo él está en condiciones de cotejar lo hecho con lo autorizado y de verificar que su orden no haya sido excedida bajo la apariencia de un hallazgo; así ocurre en las medidas intrusivas que la ley regula, en que el mismo juez que las autoriza examina cada vez la subsistencia de sus requisitos para prorrogarlas, y así lo dispone el inciso cuarto del artículo 220 cuando entrega al juez, a la vista de los objetos, la decisión sobre la legalidad de la incautación. Dejar esa verificación para el tribunal de la causa nueva significaría que el Ministerio Público podría invocar siempre un hallazgo casual y diferir el control a un juez que sólo intervendría si esa otra investigación prospera, conservando entretanto la información privada y eludiendo los resguardos aquí descritos. Cuando el Ministerio Público invoque un hallazgo, deberá explicar ante el juez que autorizó la diligencia con qué descriptor, palabra clave, interlocutor o filtro llegó a la información de que se trata, y el tribunal apreciará si esa búsqueda era razonable en relación con el objeto autorizado y con los criterios comunicados, en cuyo caso el hallazgo será casual y podrá autorizar su uso, o si se trató de una



revisión exploratoria que ninguno de esos criterios justificaba, o de criterios tan amplios que la revisión abarcó en los hechos todo el contenido, en cuyo caso la información se obtuvo fuera de los supuestos que la ley admite, no podrá utilizarse en esta ni en otra investigación y deberá eliminarse junto con el excedente de la copia. No se trata de anticipar el debate sobre exclusión de prueba de la audiencia de preparación del juicio oral, que conserva su ámbito respecto de lo que se ofrezca como evidencia en esta causa, sino de controlar la ejecución de una orden intrusiva, tarea que pertenece al juez que la dictó. Autorizado el uso, la investigación del hecho distinto seguirá su curso ante el tribunal que corresponda. El derecho comparado conoce, a título ilustrativo, exigencias semejantes, pues la Ley de Enjuiciamiento Criminal española sólo permite utilizar en otro proceso la información obtenida en una medida de investigación tecnológica dejando constancia de la solicitud inicial, de la resolución que la acordó y de sus prórrogas, y somete la continuación de la medida respecto del delito casualmente descubierto a un nuevo control judicial, según sus artículos 579 bis y 588 bis i.

Décimo sexto: Que las medidas descritas no suponen que el juez de garantía se entrometa en la investigación ni que determine qué información es útil para ella, decisión que el artículo 3° del Código Procesal Penal y el artículo 83 de la Constitución reservan al Ministerio Público. El juez no selecciona la prueba; fija las condiciones bajo las cuales una diligencia que él autorizó puede ejecutarse sin afectar más de lo necesario los derechos del imputado y de terceros, que es la función que el artículo 14 letra a) del Código Orgánico de Tribunales le asigna. No es extraño a nuestro sistema que el juez oriente de ese modo la ejecución de una diligencia. El legislador, al regular el registro remoto de equipos informáticos, exige que la resolución que lo autoriza especifique “la forma en la que se procederá al acceso y aprehensión de contenidos relevantes para la causa”, según la letra b) del artículo 225 ter, forma que el fiscal propone en su solicitud y que el juez fija y controla, sin que nadie haya visto en ello una intromisión en la dirección de la investigación. La Corte Suprema ha destacado la importancia de establecer altos estándares de exigencia respecto de la actuación de los sujetos procesales en las primeras diligencias del procedimiento, “siendo una función esencial del Juez de Control adoptar las medidas necesarias



que permitan la protección y el ejercicio de las garantías que la Constitución, las Leyes y los Tratados Internacionales otorgan a todas las personas” (SCS rol 14.900-2024, 9 de mayo de 2024). El juez que autoriza una intromisión no puede, por lo mismo, desentenderse de sus efectos. La Corte Suprema lo ha dicho al confirmar el fallo de la Corte de Valparaíso ya citado: no basta con que la judicatura haya autorizado al Ministerio Público para que la afectación del derecho sea legítima, pues “una comprensión tan acotada de la intervención judicial equivaldría a una delegación de sus facultades jurisdiccionales” y a una vulneración del mandato constitucional de reserva de ley para la afectación justificada y proporcional del derecho (SCS rol 49.866-2026, 24 de septiembre de 2026).

Tampoco altera esta conclusión la autonomía que el artículo 83 de la Constitución reconoce al persecutor, en que descansa la objeción del informe a toda limitación previa del examen, que califica de intromisión indebida en las facultades investigativas del persecutor. Esa misma norma dispone que las actuaciones que priven al imputado o a terceros del ejercicio de los derechos que la Constitución asegura, o los restrinjan o perturben, requieren de aprobación judicial previa, de modo que la intervención del juez en la delimitación de tales actuaciones no es una injerencia en la dirección de la investigación, sino el presupuesto constitucional de su legitimidad. Dirigir la investigación es decidir qué se investiga y con qué diligencias; señalar los términos en que una de ellas puede afectar la privacidad de las personas es tarea del tribunal. Por eso la Corte de Apelaciones de Valparaíso pudo observar, en el precedente citado, que el equilibrio entre los derechos de la imputada y las prerrogativas del Ministerio Público exige protocolos preestablecidos y rigurosos en el examen y traspaso de la información contenida en los dispositivos, y que su mayor especificación por la judicatura, “que es la primera llamada a asegurar el pleno respeto de las garantías de los intervinientes”, no debiera causar inquietud al persecutor.

Décimo séptimo: Que el silencio del Código Procesal Penal sobre el vaciado y revisión de teléfonos, computadores y otros equipos incautados no priva al juez de esas atribuciones ni deja la diligencia sin límites; significa sólo que éstos deben construirse desde los principios que gobiernan a todas las medidas intrusivas, esto es, la autorización judicial previa del artículo 9°,



la interpretación restrictiva del artículo 5° y la fundamentación del artículo 36, y desde la facultad que el artículo 10 confiere al juez para adoptar de oficio las medidas necesarias en cautela de las garantías. El Tribunal Europeo de Derechos Humanos, ante la ausencia de una regulación específica del acceso policial al contenido de un computador, ha exigido igualmente que el derecho interno, integrado por la jurisprudencia, imponga la autorización judicial previa y un control judicial efectivo, y ha declarado violado el Convenio cuando el examen íntegro de los archivos se practicó sin ella y sin urgencia que lo justificara (TEDH, Trabajo Rueda c. España, N° 32600/12, 30 de mayo de 2017).

Décimo octavo: Que el control descrito exige, además, una oportunidad para ejercerlo. La orden que autoriza la extracción debe señalar desde ya la audiencia en que se verificará su cumplimiento, en particular para disponer la destrucción del excedente de la copia y resolver sobre la devolución o custodia del aparato, del mismo modo que la interceptación y el registro remoto tienen una duración precisa y una prórroga sujeta a nuevo examen judicial. No basta con remitir la cuestión a la audiencia de preparación del juicio oral, como hace la resolución recurrida. La exclusión probatoria sólo operaría si el persecutor decide usar la información, en un procedimiento que puede no llegar a esa etapa y que en nada resguarda a los terceros, que no son intervinientes y jamás sabrán que sus comunicaciones fueron revisadas; y, entretanto, ni el imputado ni esos terceros tienen por qué soportar, sin una justificación que la ley no ofrece, que un órgano del Estado conserve durante meses o años, en una copia sobre la que ningún tribunal ejerce control, información sobre sus vidas que no guarda relación con el delito investigado. La retención de esos datos es por sí misma una injerencia que se prolonga en el tiempo, y no un mero antecedente de la que se produciría al usarlos; por eso el inciso cuarto del artículo 223 no espera al juicio para ordenar la destrucción de las copias de lo impertinente, y por eso los tribunales citados en el considerando décimo cuarto sitúan la eliminación inmediatamente después del examen y cuentan la injerencia desde la incautación hasta la destrucción. Una investigación de la envergadura de la presente puede prolongarse largamente antes de que se formule acusación, si es que se formula, y durante todo ese lapso, sin las



medidas que aquí se disponen, el contenido íntegro de los dispositivos permanecería a disposición del persecutor.

Décimo noveno: Que los instructivos del Ministerio Público a los que remite la resolución recurrida no bastan para conjurar la afectación descrita. El Oficio FN N° 983/2024 constituye, según sus propios términos, “normativa interna del Ministerio Público”; se aplica sólo a las causas complejas que el fiscal regional decida someter a él; confía al fiscal la evaluación inicial acerca de si la información es o no sensible y de interés investigativo; le permite considerar que toda la información de la carpeta es de interés investigativo, no sujeta a regla de protección; radica en él la decisión de anexar lo impertinente, que no se elimina sino que se guarda en custodia con un número único de evidencia, y prevé que, cuando surjan nuevas líneas de indagación, el mismo fiscal pueda estimar que lo anexado es relevante y, con autorización del fiscal regional, reincorporarlo a la carpeta. El Oficio FN N° 363/2025, por su parte, ordena a los fiscales instruir a las policías que excluyan de los informes policiales la información de la vida privada penalmente irrelevante y, si el informe la incluye, pedir una audiencia para que tales antecedentes queden reservados. Ninguno de los dos contempla la eliminación del excedente de la copia forense, ni plazos, ni un control judicial en una oportunidad determinada; la información privada e impertinente queda, en todos los casos, en poder del persecutor y bajo su exclusiva apreciación.

La misma jueza recurrida reconoció que esos instructivos dejan a salvo sólo “varias de las aprehensiones” de los litigantes y se mostró dispuesta a complementar lo resuelto para limitar o aclarar su alcance, lo que confirma que la protección quedó incompleta. Los criterios internos de actuación son valiosos, pero no sustituyen la garantía judicial, porque la decisión sobre el alcance de una injerencia en derechos fundamentales no puede quedar entregada al órgano que la ejecuta y tiene interés en su resultado. En *Särgava c. Estonia* el Tribunal Europeo estimó insuficiente que el filtrado de la copia hubiera quedado enteramente en manos de las autoridades investigadoras, y en *Nežirić c. Bosnia y Herzegovina* no bastó que los investigadores hubieran actuado concienzudamente y tratado los datos como secreto oficial, porque la búsqueda selectiva no derivaba de la ley y se practicó sin supervisión judicial. La Corte Suprema estadounidense,



en fin, frente a la propuesta del Gobierno de que las agencias desarrollaran protocolos para resolver los problemas del acceso a los datos del teléfono, observó que probablemente era una buena idea, pero que los fundadores no habían combatido una revolución para obtener el derecho a los protocolos de las agencias gubernamentales (Riley v. California, 573 U.S. 373, 398).

Vigésimo: Que no cabe acoger, en cambio, la pretensión de que se establezca un mecanismo que permita a la defensa conocer y controvertir la pertinencia de los antecedentes obtenidos de los dispositivos antes de su incorporación a la carpeta investigativa. En nuestro sistema la apreciación de qué información es útil para la investigación corresponde únicamente al Ministerio Público, que la dirige en forma exclusiva conforme a los artículos 83 de la Constitución y 3° del Código Procesal Penal y que, además, cuenta con los medios técnicos y la capacidad de análisis para efectuarla. El ordenamiento no contempla la intervención del imputado en esa selección, que sería inconciliable con el secreto que el artículo 31 de la Ley N° 19.913 impone a una indagación reservada como la presente, según se consignó en la audiencia, y que en los hechos le permitiría conocer por anticipado la evidencia reunida en su contra. Lo que el juez puede y debe hacer es fijar los límites de la búsqueda, recibir del persecutor los criterios con que la practicará, apreciar si son razonables y controlar después su cumplimiento, no ejecutarla ni sustituir al persecutor en la selección de la evidencia; la defensa será oída en la audiencia en que ese control se ejerza, como se dispondrá, sin perjuicio de la exclusión probatoria que pueda pedir en su oportunidad. Tampoco se trata, como temió la recurrida, de dejar la entrega de la información al arbitrio de la persona investigada, pues los criterios los propone el persecutor y los aprueba el juez, sin que el imputado intervenga en su definición.

Vigésimo primero: Que, el artículo 220 del Código Procesal Penal, que el recurso invoca junto con el artículo 218 como límite objetivo de la revisión, no ofrece la solución del caso. Esta norma impide incautar las comunicaciones entre el imputado y las personas que pueden abstenerse de declarar por parentesco, conforme al artículo 302, o por razón de secreto, conforme al artículo 303, así como las notas y documentos a que se extiende esa facultad, pero su inciso segundo dispone que esas



limitaciones “sólo regirán” cuando tales objetos “se encontraren en poder de las personas a quienes la ley reconoce la facultad de no prestar declaración”, y las extiende a las oficinas o establecimientos de los profesionales del artículo 303. La norma protege, entonces, la confianza que el imputado deposita en su pariente, su abogado, su médico o su confesor, y lo hace impidiendo que lo confiado se incaute en manos de estos últimos; su ámbito propio sería el teléfono, el dispositivo o los papeles del abogado defensor del amparado, en los que constaran las consultas o la asesoría de su defensa, y no el caso de autos, en que lo incautado son los dispositivos del imputado mismo, pues la norma no establece una prohibición general de incautar sus comunicaciones dondequiera que se encuentren, en lo que la recurrida tiene razón. El artículo 218, por su parte, regula la retención e incautación de la correspondencia dirigida al imputado o remitida por él y la obtención de copias de su correspondencia electrónica, y su exigencia de que por motivos fundados sea previsible su utilidad para la investigación se refiere a la autorización de la diligencia, que aquí se concedió por la resolución de 19 de agosto; pero la misma norma ordena al fiscal examinar lo retenido, conservar sólo lo que tenga relación con el hecho investigado y devolver lo demás, regla que, lejos de oponerse a las medidas que se han descrito, confirma que la ley no admite que el persecutor retenga indefinidamente lo que no guarda relación con los hechos.

Descartado que el artículo 220 sea aplicable al caso de autos, y para mayor claridad de lo que se resolverá, conviene entonces distinguir tres situaciones.

La primera es la de las comunicaciones que el amparado, en cuanto imputado, haya mantenido con sus abogados defensores, en esta o en otras causas judiciales, para preparar y ejercer su defensa. Están protegidas, aunque no específicamente por el artículo 220, sino por el derecho a la defensa que aseguran el artículo 19 N° 3 de la Constitución, el artículo 8° del Código Procesal Penal y los tratados recordados en el considerando noveno, y por la misma razón que lleva al inciso tercero del artículo 222 a prohibir la interceptación de las comunicaciones entre el imputado y su abogado, salvo que el juez estime fundadamente que éste pudiere tener responsabilidad penal en los hechos investigados. Por eso, si los dispositivos las contienen, deben quedar excluidas de la búsqueda y



eliminarse de la copia, aun cuando los criterios de búsqueda las alcancen, a menos que el abogado de que se trate sea también imputado por los hechos investigados, lo que no se ha planteado respecto de los abogados que asumen la defensa del amparado.

La segunda es la de las comunicaciones del amparado con su cónyuge, sus hijos y otras personas ajenas a los hechos, y la de los documentos sobre su salud y sobre consultas legales que nada tienen que ver con su defensa, a los que el recurso alude. Su protección, como se dijo, no proviene del artículo 220, sino de la garantía que los numerales 4° y 5° del artículo 19 de la Constitución dispensan a toda comunicación y a toda forma de vida privada, del amparado y de esos terceros, respecto de información ajena a los hechos investigados a la que, como la propia recurrida admite, el persecutor tendrá acceso. Ese criterio, la impertinencia de la información, cubre por igual las comunicaciones con familiares, amigos o cualquier otra persona, es el que subyace a lo dicho en el considerando noveno y justifica que se ordene excluirlas de la búsqueda y eliminarlas de la copia.

La tercera es la de las comunicaciones con esas mismas personas que sí se relacionan con los delitos investigados. No cabe excluirlas de antemano en bloque, porque los criterios de búsqueda, determinados por los hechos, las personas y la época de interés, pueden conducir a intercambios que el amparado sostuvo con un pariente o con otra persona de su confianza y que conciernen a esos hechos; si quedan comprendidas en esos criterios, y dado que el amparado es imputado, tales comunicaciones son pertinentes, y la facultad de abstenerse de declarar que los artículos 302 y 303 reconocen al pariente o al profesional no crea, sobre los registros que el imputado guarda en sus dispositivos, una zona inmune a la investigación que se sigue en su contra, de suerte que pueden ser examinadas, conservadas y utilizadas. En lo que la recurrida acertó fue en reconocer, en su informe, que los resguardos que adoptó se aplican también a las comunicaciones familiares del amparado y a las sostenidas con personas obligadas al secreto; lo que faltó fue hacerlos efectivos con medidas concretas.

Vigésimo segundo: Que tampoco puede prosperar la petición de que se dé a la defensa acceso a la parte de la carpeta judicial electrónica que se



mantiene reservada y copia de la solicitud en que el Ministerio Público fundó las medidas intrusivas. El artículo 31 de la Ley N° 19.913 dispone que la investigación de los delitos de lavado de activos será secreta respecto del imputado y de los demás intervinientes cuando así lo disponga el fiscal, por un plazo máximo de seis meses renovable por una vez con autorización del juez de garantía, y sólo permite al imputado pedir que se limite el secreto en cuanto a las piezas o actuaciones abarcadas por él una vez formalizada la investigación; su inciso final sanciona, además, a quien entregue o difunda “información de cualquier naturaleza acerca de antecedentes de la investigación”. Lo que la ley reserva son, pues, los antecedentes de la investigación, cualquiera sea el soporte o el registro en que se encuentren. La solicitud de medidas intrusivas los contiene, porque el artículo 9° del Código Procesal Penal obliga al fiscal a exponerlos al juez para obtener la autorización, y el artículo 236 permite que la diligencia se practique sin conocimiento del afectado, como aquí ocurrió. Incorporada esa solicitud a la carpeta judicial, no cambia de naturaleza. Si el acceso a esa carpeta bastara para conocerla, la reserva del artículo 31 quedaría sin aplicación en los casos en que el fiscal necesita la intervención del juez, que son los de mayor intensidad investigativa, y el secreto de una investigación reservada cedería ante la publicidad que el artículo 2° letra c) de la Ley N° 20.886 establece para la carpeta electrónica “salvo las excepciones establecidas por la ley”, publicidad que esa misma norma restringe respecto de las presentaciones sobre medidas cautelares y otras materias cuya eficacia requiera de reserva. El artículo 31 es una de esas excepciones legales y, en cuanto norma especial, prevalece tanto sobre la regla general de publicidad de la Ley N° 20.886 como sobre el régimen ordinario de secreto del artículo 182 del Código Procesal Penal. No hay en ello analogía ni interpretación extensiva, sino aplicación directa de la norma a su objeto, los antecedentes de la investigación, que no dejan de serlo por reproducirse en una pieza de la carpeta judicial ni por ser anteriores a la decisión del fiscal que dispuso la reserva, de modo que no se infringe el inciso segundo del artículo 5° del Código.

El precedente de la Corte Suprema que el recurso invoca no conduce a otra conclusión. En él se acogió el amparo de un imputado a quien se había negado el acceso a la carpeta judicial electrónica por la vía de aplicar



a ella el secreto de la carpeta investigativa, pero se dispuso al mismo tiempo que el juzgado de garantía adoptara las medidas pertinentes para que ese acceso no colisionara ni entorpeciera las diligencias o registros de la carpeta investigativa sobre los que estuviera vigente el secreto (SCS rol 34.081-2025, 29 de agosto de 2025), que es lo que la recurrida resolvió, pues no negó a la defensa el acceso a la carpeta judicial, sino a las piezas que reproducen los antecedentes reservados. Los fallos relativos al secreto del artículo 38 de la Ley N° 20.000 tampoco favorecen al recurrente, ya que en ellos se reprochó al juez de garantía haber renunciado a ejercer el control que le corresponde, al tener por privativa del persecutor una atribución que debe ejercerse proporcionalmente, y haber privado a la defensa de los antecedentes mínimos para debatir la prisión preventiva de los amparados (SCS rol 15.398-2025, 14 de mayo de 2025; SCS rol 58.100-2025, 13 de enero de 2026), situación distinta de la de autos, en que no se discute una medida cautelar personal, la jueza resolvió la petición de la defensa en audiencia y por decisión fundada, y la ley señala la oportunidad en que el imputado puede pedir que el secreto se limite.

Vigésimo tercero: Que, por lo mismo, la negativa de acceso no priva a la resolución de 19 de agosto de 2026 del fundamento que los artículos 9° y 36 del Código Procesal Penal exigen ni deja a la defensa sin posibilidad de control. Esa resolución no se limita a remitirse a antecedentes que no expresa. Identifica los delitos investigados; describe los hechos, esto es, las irregularidades de la empresa proveedora en la ejecución de contratos del Programa de Alimentación Escolar, el soborno y cohecho de funcionarios públicos para favorecer a esa empresa en la obtención de información reservada y en la adjudicación de licitaciones, y el mecanismo sostenido en el tiempo en que participarían directivos de la empresa, lobistas, funcionarios de la Junta Nacional de Auxilio Escolar y Becas y parlamentarios; señala la clase de antecedentes reunidos y las diligencias previas que los aportaron, y precisa los objetos cuya incautación autoriza y su relación con los hechos, de modo que el amparado conoce la imputación en los términos en que el secreto lo permite. Lo que el recurso echa de menos es el detalle de esos antecedentes, que es justamente lo que la ley reserva por un tiempo, y el control de la ejecución de la diligencia, que es lo que esta sentencia establece. Cuando la reserva termine, o cuando el juez



de garantía la limite a petición del imputado una vez formalizada la investigación, la defensa podrá examinar la solicitud y controvertir, si lo estima, la concurrencia de los presupuestos de la autorización. En cuanto a la falta de límites de esa resolución, que el recurso también reprocha, no se requiere un pronunciamiento separado, pues las medidas que se dispondrán rigen la ejecución de la revisión que ella autorizó y complementan, con ese alcance, la resolución de 26 de agosto que se pronunció sobre la cautela pedida. Por último, la constancia de la autorización verbal para el registro de la oficina del amparado en Santiago, cuya autenticidad el recurso pone en duda por carecer de firma, fue acompañada al informe suscrita con la firma electrónica de la jueza que la otorgó, lo que despeja esa objeción.

Vigésimo cuarto: Que lo que se resolverá no busca limitar ni obstaculizar la investigación del Ministerio Público, sino alcanzar el equilibrio entre la eficacia de la persecución penal y el respeto de los derechos fundamentales que la Constitución exige en toda diligencia intrusiva. La extracción y el análisis del contenido de los dispositivos podrán continuar; la delimitación de los hechos, del período y de las personas de interés seguirá siendo propuesta por el persecutor; y ningún antecedente pertinente a los hechos investigados quedará fuera de su alcance. Lo único que se agrega es aquello que el legislador ya impone a diligencias de intensidad comparable, esto es, un plazo, un objeto determinado, la destrucción de lo que no sirve y una oportunidad para que el juez verifique que así se hizo. Ese es el sentido del artículo 10 del Código Procesal Penal cuando faculta al juez para adoptar las medidas necesarias para el ejercicio de las garantías, y del artículo 14 letra a) del Código Orgánico de Tribunales cuando le encomienda asegurarlas. Esta Corte no desconoce que se trata de un control que los tribunales no han practicado, o sólo excepcionalmente, respecto de una diligencia que la ley no regula. Por eso las medidas que se adoptan son las que parecen razonables y prudentes para restablecer el equilibrio buscado, en la expectativa de que resulten suficientes; pero, dada la dificultad de la materia, el mismo juzgado de garantía podrá revisarlas, de oficio o a petición de cualquier interviniente, cuando su ejecución muestre que son insuficientes para proteger los derechos comprometidos o que



entorpecen innecesariamente la investigación, y hacer los ajustes que ese equilibrio requiera.

Vigésimo quinto: Que, conforme a lo razonado, la resolución de 26 de agosto de 2026, en cuanto rechazó fijar límites a la ejecución de la extracción y revisión de los dispositivos del amparado más allá de los que consignó, y remitió el resguardo de la información impertinente y privada a instructivos internos del persecutor y a una eventual exclusión probatoria futura, no satisfizo las exigencias que los artículos 5°, 9°, 10 y 36 del Código Procesal Penal y 14 letra a) del Código Orgánico de Tribunales imponen al juez de garantía, y dejó subsistente una afectación cierta y actual de la vida privada del amparado y de la inviolabilidad de sus comunicaciones y de las de terceros, sobre la cual, conforme a lo resuelto por la Corte Suprema, corresponde a esta Corte pronunciarse derechamente, y que debe hacer cesar. En un caso semejante, el máximo tribunal ha estimado que exponer a la imputada a pesquisas investigativas sin la adopción de medidas de contrapeso que resguarden sus garantías fundamentales amenaza indebidamente su libertad personal y afecta de manera ostensible su derecho a la intimidad (SCS rol 49.866-2026, 24 de septiembre de 2026). Las medidas que se dispondrán siguen las líneas de ese precedente, con el apoyo que la regla del inciso cuarto del artículo 223 presta a la eliminación del excedente de la copia, y agregan la fijación de un plazo y de una audiencia de control. La identificación de la información útil deberá completarse dentro de noventa días contados desde la notificación de esta sentencia, plazo que sólo podrá ampliarse por una vez, por resolución fundada dictada en audiencia, para que por esa vía no se eluda el control ni se prolongue la conservación de la copia; y la audiencia en que se verificará lo obrado y se dispondrá la eliminación se celebrará dentro de los diez días siguientes, con citación de la defensa del amparado. La reserva de la investigación decretada con arreglo al artículo 31 de la Ley N° 19.913 no es obstáculo para ello. Esa norma, como se dijo, permite mantener en secreto la investigación respecto del imputado, pero la audiencia versará sobre la conservación de la copia del contenido de sus propios dispositivos, que él obviamente conoce, y sobre los descriptores con que se acota la búsqueda y la información que se estima impertinente, cuya revelación no compromete de modo relevante el secreto ni el éxito de la investigación,



menos aún cuando los delitos que se indagan constan en los escritos públicos de este amparo y las defensas conocen los hechos desde la audiencia de cautela de garantías. Diferir el control hasta el término de la reserva, que puede extenderse por un año, sería una forma de eludirlo. Durante ese plazo el persecutor y la policía trabajarán sobre la copia íntegra para identificar lo pertinente; completada la identificación, y hasta que la audiencia resuelva sobre la eliminación, la copia quedará sellada y sin acceso, porque desde ese momento el examen ha concluido y el persecutor sólo necesita la información que separó como relacionada con los hechos, de modo que en el lapso que media entre el término del examen y la audiencia la retención deja de ser una intromisión en curso.

Así, el amparo será acogido sólo en cuanto se dispondrán las medidas de control que se indicarán, y rechazado en lo demás, sin costas.

Por estas consideraciones y de conformidad, además, con lo dispuesto en el artículo 21 de la Constitución Política de la República y en el Auto Acordado de la Excma. Corte Suprema sobre Tramitación y Fallo del Recurso de Amparo, **se acoge**, sin costas, el recurso de amparo deducido por Alejandro Espinoza Bustos e Ignacio Sotomayor Uribe en favor de Sergio Alfredo Gahona Salazar, en contra del Cuarto Juzgado de Garantía de Santiago, sólo en cuanto se declara que la resolución dictada el 26 de agosto de 2026 en la causa RUC 2600858361-6, RIT O-6719-2026, debe complementarse con las siguientes medidas, que dicho tribunal deberá adoptar y controlar:

a) El Ministerio Público informará al Cuarto Juzgado de Garantía de Santiago, dentro de quince días, el estado de la extracción y de la revisión ya practicada, la individualización de los funcionarios y peritos que han tenido y tendrán acceso a las copias obtenidas de los dispositivos incautados al amparado, y propondrá los criterios de búsqueda con que se practicará el análisis de la totalidad de lo extraído, incluidas las comunicaciones de las aplicaciones de mensajería, del correo electrónico y de las redes sociales, sean palabras clave, interlocutores, cuentas, tipos de archivo u otros descriptores, determinados por los hechos investigados, por el período comprendido entre el año 2018 y el 20 de agosto de 2026 ya fijado en la resolución recurrida y por las personas, números o cuentas de interés para la investigación, sin perjuicio de su posterior complementación



con conocimiento del tribunal. Las comunicaciones alcanzadas por los criterios de búsqueda, por relacionarse con los hechos investigados, podrán ser examinadas y conservadas cualquiera sea su interlocutor. Quedarán excluidas de la búsqueda, y serán eliminadas de la copia, las comunicaciones del amparado con sus abogados defensores, en esta o en otras causas, relativas al ejercicio de su defensa, a menos que el abogado respectivo fuere imputado por los hechos investigados. El juez de garantía apreciará la precisión y razonabilidad de los criterios propuestos y podrá exigir su acotamiento. Los dispositivos incautados y las copias obtenidas de ellos permanecerán bajo la custodia exclusiva del fiscal adjunto a cargo de la investigación.

b) La identificación de la información útil para la investigación deberá completarse dentro de noventa días contados desde la notificación de esta sentencia. El juez de garantía podrá ampliar ese plazo por una sola vez, por resolución fundada dictada en audiencia a la que se citará a la defensa del amparado, previo informe del Ministerio Público sobre el estado de la diligencia; la ampliación no suspenderá las demás medidas de esta sentencia. Vencido el plazo o su ampliación, el Ministerio Público separará en un soporte distinto la información identificada como relacionada con los hechos investigados e informará de ello al tribunal, y la copia íntegra de cada dispositivo quedará desde entonces sellada, bajo la custodia del fiscal a cargo conforme al artículo 188 del Código Procesal Penal, sin acceso alguno hasta que el tribunal resuelva sobre su eliminación.

c) Dentro de los diez días siguientes al vencimiento del plazo de la letra b) o de su ampliación, el Cuarto Juzgado de Garantía de Santiago celebrará una audiencia, con citación de la defensa del amparado, en la que el Ministerio Público dará cuenta de la información que conservará por tener relación con los hechos investigados, incluida, en su caso, la obtenida a través de las cuentas abiertas en los dispositivos a que se refiere la letra f), y en la que el tribunal dispondrá la eliminación de la copia íntegra sellada y de toda otra información extraída que no haya sido identificada como pertinente, en particular la relativa a las comunicaciones del amparado con sus abogados defensores a que se refiere la letra a), de lo que deberá dejarse constancia mediante certificación que identifique el procedimiento seguido y a los funcionarios que lo practicaron, y resolverá sobre la



devolución de los dispositivos al amparado o, si su conservación fuere necesaria, sobre su custodia. La reserva de la investigación decretada conforme al artículo 31 de la Ley N° 19.913 no suspenderá esta audiencia ni la intervención de la defensa del amparado en ella.

d) Hasta que se celebre esa audiencia, el Ministerio Público podrá utilizar en la investigación únicamente la información que identifique como relacionada con los hechos investigados. La información restante no podrá ser examinada más allá de lo necesario para su identificación, ni entregada a otros intervinientes o a terceros, ni incorporada a la carpeta investigativa ni a informes policiales, conforme a lo ya resuelto por el tribunal recurrido, y quedará comprendida en la copia sellada a que se refiere la letra b).

e) Si el Ministerio Público estimare que la copia contiene información relevante para hechos distintos de los investigados, deberá ponerlo en conocimiento del Cuarto Juzgado de Garantía de Santiago antes de utilizarla con cualquier fin, indicando el criterio o descriptor de búsqueda con que llegó a ella. El tribunal, con los criterios informados conforme a la letra a), verificará si se trató de un hallazgo casual, producido dentro de los límites de la orden y de una búsqueda razonable, y no de una revisión exploratoria del contenido en busca de delitos no determinados. Si lo estima así, autorizará su uso; en caso contrario, la información no podrá utilizarse en esta ni en otra investigación y será eliminada junto con el excedente de la copia conforme a la letra c). En caso de urgencia, la autorización podrá requerirse por la vía más rápida.

f) Las limitaciones anteriores rigen respecto de la totalidad de la información extraída, esté almacenada en los dispositivos o se obtenga desde servidores externos a través de las aplicaciones y cuentas abiertas en ellos, y en particular respecto de las aplicaciones de mensajería, del correo electrónico, incluidas las cuentas institucionales del amparado a las que la resolución de 19 de agosto de 2026 autorizó acceder, de las redes sociales y de los servicios de almacenamiento en la nube. Los criterios de búsqueda de la letra a) deberán determinar, para cada una de esas aplicaciones y servicios, las cuentas, los interlocutores o contactos y el período cuyas comunicaciones o contenidos podrán examinarse, y las palabras clave o categorías de contenido a que se acotará la revisión, sin que puedan examinarse íntegramente conversaciones, casillas, perfiles o



repositorios de personas ajenas a los hechos investigados. En cuanto al acceso, a través de los dispositivos, a los servicios en línea que el amparado mantiene con la cuenta abierta, esto es, el correo electrónico, las redes sociales, la mensajería sincronizada y el almacenamiento en la nube, cuya información no está necesariamente grabada en los aparatos sino en servidores externos, pero a la que se llega directamente desde ellos, acceso que la resolución de 19 de agosto de 2026 autorizó en términos genéricos, el Ministerio Público informará además al tribunal, en el plazo de la letra a), a qué servicios y cuentas ha accedido o pretende acceder por esa vía, para que el juez de garantía determine el alcance de ese acceso con arreglo a los artículos 225 bis, 225 ter y 225 quáter del Código Procesal Penal; fuera de lo así informado y autorizado, no podrá accederse a esos servicios ni a la información guardada en sus servidores a través de los dispositivos.

g) Las fotografías, videos y audios contenidos en los dispositivos o accesibles a través de las cuentas abiertas en ellos, cuyo contenido no puede seleccionarse mediante palabras clave, se examinarán con sujeción al período fijado y a su procedencia, ordenando la revisión a partir de los archivos adjuntos a las conversaciones, correos o cuentas comprendidos en los criterios de búsqueda. Dentro de ese universo la revisión será directa y la practicarán únicamente los funcionarios individualizados conforme a la letra a), sin generar copias adicionales, dejando constancia de los archivos que se conserven por su relación con los hechos investigados; los restantes, incluidos los de carácter personal y familiar, quedarán comprendidos en la eliminación de la letra c).

h) El Cuarto Juzgado de Garantía de Santiago podrá, de oficio o a petición de cualquier interviniente y por resolución fundada dictada en audiencia, ajustar las medidas anteriores cuando su ejecución muestre que resultan insuficientes para resguardar los derechos comprometidos o que entorpecen innecesariamente la investigación.

Regístrese, notifíquese y archívese.

Redacción del ministro Manuel Rodríguez Vega.

Amparo N° 4268-2026.-

No firma la ministra señora Rodríguez Fondón, no obstante haber concurrido a la vista y al acuerdo del fallo, por estar haciendo uso del permiso del artículo 347 del Código Orgánico de Tribunales.



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: QWDJDZLUUP



Manuel Esteban Rodríguez Vega

Ministro

Corte de Apelaciones

Veintinueve de septiembre de dos mil veintiséis
13:08 UTC-3



Carolina Sandra Brengi Zunino

Ministro

Corte de Apelaciones

Veintinueve de septiembre de dos mil veintiséis
13:04 UTC-3



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: QWDJDXLZUUP

Pronunciado por la Sexta Sala de la C.A. de Santiago integrada por los Ministros (as) Manuel Esteban Rodríguez V., Carolina S. Brengi Z. Santiago, veintinueve de septiembre de dos mil veintiseis.

En Santiago, a veintinueve de septiembre de dos mil veintiseis, notifiqué en Secretaría por el Estado Diario la resolución precedente.



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: QWDJDXLZUUP

Santiago, veintinueve de septiembre de dos mil veintiséis.

Vistos y teniendo presente:

Primero: Que comparece el abogado Samuel Donoso Boassi, en representación de Darío Calderón González, abogado, e interpone acción constitucional de amparo en su favor en contra del Cuarto Juzgado de Garantía de Santiago, por dos resoluciones dictadas en la causa RUC 2600858361-6, RIT O-6719-2026, esto es, la de 19 de agosto de 2026, de la jueza Francis Patricia Fell Franco, que autorizó la incautación de sus dispositivos electrónicos y el acceso, extracción, revisión y análisis de “toda la información” contenida en ellos, y la de 26 de agosto de 2026, dictada por la jueza Daniela Verónica Guerrero González en la audiencia de cautela de garantías promovida por su defensa, que rechazó limitar ese acceso mediante criterios de pertinencia por fechas, materias y personas.

Sostiene que ambas resoluciones son ilegales y arbitrarias y que amenazan y perturban la libertad personal y la seguridad individual del amparado, garantizadas en el artículo 19 N° 7 de la Constitución Política de la República, en relación con el procedimiento racional y justo, el respeto a la vida privada y la inviolabilidad de las comunicaciones privadas que aseguran los numerales 3°, 4° y 5° del mismo artículo.

En cuanto a los hechos, expone que la Fiscalía de Alta Complejidad Oriente del Ministerio Público sigue una investigación en la que ni el amparado ni su defensa conocen los hechos concretos que se le atribuyen, los delitos que se le imputan ni las fechas en que se habrían cometido, lo que tampoco se desprende de la resolución de 19 de agosto de 2026. Según ésta, el Ministerio Público sostiene que la empresa SOSER S.A. habría incurrido en graves irregularidades en la ejecución de contratos de licitación pública para la prestación de servicios de alimentación a establecimientos educacionales de la región de O'Higgins, y en delitos reiterados de soborno y cohecho a funcionarios públicos para obtener información reservada y la adjudicación de licitaciones, en una investigación que comprende delitos de fraude al fisco, fraude informático, delitos contra la salud pública, falsificación de instrumento privado, cohecho y lavado de activos. A petición de la fiscal adjunta, el tribunal autorizó ese día la entrada y registro de ocho domicilios y la incautación de teléfonos celulares, computadores, discos duros y demás dispositivos de almacenamiento digital



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: GFPDXZYNUP

que pudieran dar cuenta de reuniones, intercambios de información y otras formas de comunicación relacionadas con los hechos investigados, tanto respecto de las personas asociadas a esos domicilios como de otras ocho, entre ellas el amparado, en su calidad de ex presidente de la asociación gremial Nutre Chile. La diligencia se ejecutó al día siguiente y en ella se incautaron desde su domicilio, entre otras especies, su teléfono celular personal, el computador personal de su casa, un iPad y el computador de su oficina, que hubo de mandar a buscar.

Agrega que, en la misma resolución, el tribunal autorizó al persecutor y a la policía el acceso, revisión, extracción y análisis de “toda la información” contenida en las especies incautadas, esto es, sus memorias internas y externas, la tarjeta SIM, las imágenes, videos, audios y todo dato y registro almacenado en ellas, así como en sus aplicaciones, redes sociales, correos electrónicos y nubes de almacenamiento vinculadas, incluidos los mensajes de las aplicaciones instaladas, los registros de llamadas, los registros de audio y la geolocalización, sin fijar un rango temporal de búsqueda, sin identificar a las personas cuyas comunicaciones interesan a la investigación, sin disponer un método de búsqueda dirigida por descriptores o palabras clave y sin establecer mecanismo alguno de segregación, devolución o destrucción de lo impertinente, ni análisis propio de pertinencia, necesidad o proporcionalidad, en contradicción con el marco que la propia resolución fijó para la incautación. Lo autorizado no sería, a su juicio, una diligencia determinada sobre objetos determinados, sino una habilitación abierta para explorar la totalidad de su acervo digital. Por ello su defensa promovió una audiencia de cautela de garantías conforme al artículo 10 del Código Procesal Penal, celebrada el 26 de agosto de 2026, en la que pidió que el tribunal delimitara el acceso mediante criterios objetivos de pertinencia referidos a los hechos investigados, al período en que se sitúan y a las personas de interés para la investigación, solicitud que fue rechazada, con lo que, afirma, se agotó la única vía ordinaria de que disponía para obtener la delimitación de la medida. Añade que la lesión no es hipotética, pues la autorización se encuentra vigente y en ejecución, y que una vez que el contenido íntegro sea copiado, examinado e incorporado a la carpeta investigativa el conocimiento estatal y de terceros sobre su vida privada será un hecho consumado e irreversible.



En cuanto al derecho, sostiene que el amparo es procedente porque la libertad personal y la seguridad individual pueden verse afectadas por vía consecuencial, con ocasión de la ejecución de un acto lesivo de otros derechos, como lo ha declarado la Corte Suprema al acoger amparos deducidos contra resoluciones de jueces de garantía que autorizaron medidas intrusivas sobre dispositivos electrónicos en los roles 14.900-2024, 12.292-2025 y 16.420-2025, y porque lo impugnado no es una actuación del Ministerio Público sino resoluciones del propio juez de garantía llamado a ejercer el control, que, requerido dos veces, no lo ejerció. Afirma que la resolución de 19 de agosto de 2026 constituye una orden general de registro digital, pues un teléfono contemporáneo contiene de manera agregada y retrospectiva la vida entera de una persona y, en el caso de un abogado, comunicaciones amparadas por el secreto profesional, y que sin una delimitación previa del objeto del registro toda incautación de un dispositivo se transforma en una búsqueda general en el acervo digital de la persona, como advierte la doctrina que cita. Agrega que ninguna norma habilita un registro general del contenido de un dispositivo incautado, ya que el artículo 218 bis del Código Procesal Penal sólo regula la preservación provisoria de datos en poder de proveedores de servicios, de modo que el tribunal extendió por analogía una habilitación que la ley no contempla, en contra de lo que dispone el inciso segundo del artículo 5° del mismo Código. Denuncia, además, la falta de fundamentación de esa resolución, con infracción de sus artículos 9° y 36, porque su única motivación sería la remisión al mérito de los antecedentes contenidos en la solicitud de la fiscal y a lo que constaría en las anteriores solicitudes del Ministerio Público y en las resoluciones de 9, 14 y 15 de julio de 2026 que autorizaron otras diligencias intrusivas, cuyo contenido la defensa desconoce por la reserva decretada, técnica de fundamentación por reenvío que la Corte Suprema habría censurado en los fallos citados y la Corte de Apelaciones de Antofagasta en el Rol N° 282-2025, sin que la motivación pueda construirse a posteriori en el informe que se evacue ante esta Corte.

Invoca los artículos 19 N° 3, 4 y 5 de la Constitución, 11 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos, y el secreto profesional del abogado, reconocido en el artículo 360 del Código de Procedimiento Civil,



en los artículos 217, 220 y 303 del Código Procesal Penal y en el artículo 64 del Código de Ética Profesional del Colegio de Abogados, cuyo valor normativo y vinculación con el derecho de defensa la Corte Suprema habría reconocido en los fallos que cita. Sostiene que la resolución infringe el artículo 218 del Código Procesal Penal, que sólo permite conservar la correspondencia relacionada con el hecho investigado y ordena devolver la restante; el artículo 220, en relación con los artículos 302 y 303, que prohíbe incautar las comunicaciones entre el imputado y las personas que pueden abstenerse de declarar y ordena entregar selladas al juez las de calificación dudosa, prohibición que sólo un mecanismo de exclusión previo al conocimiento del equipo investigador haría efectiva; y el artículo 223, que ordena destruir los registros de las comunicaciones impertinentes, normas de las que extrae que el Estado no puede retener ni examinar material comunicacional impertinente. Afirma que la medida no supera el juicio de proporcionalidad, pues la información ajena a los hechos nada aporta a la investigación, existe una alternativa menos lesiva e igualmente eficaz, consistente en la búsqueda dirigida por fechas, materias y personas con segregación de lo impertinente, y el sacrificio impuesto es superior al beneficio persecutorio. Que esa alternativa es practicable lo demostrarían el protocolo de acceso que el Séptimo Juzgado de Garantía de Santiago fijó el 13 de marzo de 2025 en la investigación seguida contra la senadora Karol Cariola y la sentencia de la Corte de Apelaciones de Valparaíso de 1 de septiembre de 2026, Rol N° 3810-2026, que acogió el amparo deducido en favor de la senadora Camila Flores y fijó los límites a que debe ceñirse el examen de los dispositivos incautados. Precisa que no pide dejar sin efecto la incautación, impedir el acceso del Ministerio Público al contenido de las especies ni su restitución, sino que el acceso quede circunscrito a lo que la investigación requiere.

Pide que se acoja el amparo y se declare que la resolución de 19 de agosto de 2026 es ilegal y arbitraria en cuanto autoriza el acceso, extracción, revisión y análisis de toda la información contenida en las especies incautadas, sin límite ni resguardo alguno y sin la fundamentación exigida, y que igualmente lo es la de 26 de agosto de 2026, que rechazó delimitar ese acceso; que se deje sin efecto la autorización en cuanto ilimitada y se circunscriba el acceso a las comunicaciones, archivos y datos



del período en que se sitúan los hechos investigados, a las materias vinculadas a esos hechos, con exclusión de los contenidos de carácter familiar, conyugal, íntimo, de salud, patrimonial ajeno a los hechos y de las comunicaciones propias de la función de abogado no vinculadas a ellos, y a las comunicaciones mantenidas con personas que revistan interés para la investigación o que el Ministerio Público individualice fundadamente y el juzgado apruebe, oída la defensa; que la extracción y el examen se practiquen mediante búsquedas dirigidas por palabras clave, descriptores y rangos de fechas aprobados previamente por el Cuarto Juzgado de Garantía de Santiago, a propuesta del Ministerio Público y oída la defensa, con prohibición de toda exploración fuera de esos parámetros; que se excluyan del acceso y del análisis las comunicaciones del amparado con su cónyuge, parientes, abogados y demás personas comprendidas en el artículo 302 del Código Procesal Penal, entregándose selladas al juez de garantía las de calificación dudosa; que se le devuelva la información y las especies sin relación con el hecho investigado y se destruyan las copias que de ellas se hubieren obtenido; y que se ordene al tribunal, por un juez que no hubiere dictado las resoluciones recurridas, fiscalizar el cumplimiento de lo resuelto, con costas.

Segundo: Que Daniela Verónica Guerrero González, jueza titular del Cuarto Juzgado de Garantía de Santiago, evacuó el informe que le fue requerido y sostuvo que la resolución de 26 de agosto de 2026 se ajusta a la normativa procesal vigente y que no se verifica la ilegalidad y arbitrariedad denunciadas.

Expone que en la audiencia de esa fecha, celebrada para controlar las garantías de los imputados conforme al artículo 10 del Código Procesal Penal, las defensas de cuatro investigados, entre ellas la del amparado, pidieron copia de la solicitud que motivó la resolución de 18 de agosto de 2026 y que se regulara judicialmente el acceso del Ministerio Público y de las policías a los dispositivos electrónicos incautados, a lo que el persecutor se opuso. Preciso que ninguna de esas alegaciones pretendía impugnar los fundamentos de la resolución que se pronunció sobre las medidas intrusivas. El tribunal rechazó la entrega de copias, por tratarse de antecedentes de la investigación sujetos a la reserva decretada por el Ministerio Público el 24 de julio de 2026 con arreglo al artículo 31 de la Ley



N° 19.913, aunque se encuentren en la carpeta judicial, y razonó que toda medida intrusiva afecta derechos y garantías, motivo por el cual exige autorización judicial previa, la que en este caso se dictó el 18 de agosto de 2026, y que la naturaleza de los delitos de corrupción explica que tales autorizaciones se otorguen sin conocimiento del afectado y en una investigación reservada.

Descartó luego la aplicación del artículo 220 del Código Procesal Penal al abogado que tiene la calidad de imputado, sin perjuicio de precisar que no es parte de la investigación indagar en las comunicaciones que en esa calidad mantenga con sus clientes, las que estarán a resguardo en la medida en que no se relacionen con los hechos investigados. Estimó que no es posible una exclusión *ex ante* de parte de la información, que la entrega de ésta no puede quedar al arbitrio de la persona investigada y que limitar el examen conforme a criterios previos importaría una intromisión indebida en las facultades del persecutor y entorpecería el análisis, quedando a salvo la posibilidad de solicitar en su oportunidad la exclusión del medio probatorio. Reconoció, con todo, que el persecutor tendrá acceso a información impertinente y privada y que no es posible limitar esa posibilidad sin riesgo de frustrar la investigación.

En consecuencia, acogió la segunda solicitud sólo en cuanto la búsqueda de la información relativa a los hechos investigados deberá circunscribirse al período comprendido entre el año 2018 y el 20 de agosto de 2026, fecha de la incautación; prohibió la entrega a los intervinientes o a terceros, y la incorporación a la carpeta investigativa, de toda información contenida en los dispositivos ajena a los hechos; y ordenó al Ministerio Público sujetar su actuación a los instructivos contenidos en sus oficios 363/2025 y 983/2024, respecto de los cuales advirtió que dejan a salvo varias de las aprehensiones de los litigantes y que el tribunal no tenía inconveniente en que se plantearan complementaciones destinadas a limitar o aclarar el alcance de lo resuelto.

En cuanto al derecho, afirma que la lectura que el recurso hace de los artículos 218, 220 y 223 del Código Procesal Penal no resiste el análisis de su propio tenor. El inciso final del artículo 218, al ordenar al fiscal conservar sólo la correspondencia relacionada con el hecho investigado y devolver la restante, presupone un examen previo del contenido, pues no es posible



discernir lo pertinente sin haber accedido a él, de modo que establece un estándar de custodia y restitución posterior al examen y no una prohibición de examinar; el régimen de entrega sellada del artículo 220, en relación con los artículos 302 y 303, es una regla especial para las comunicaciones con personas que pueden abstenerse de declarar y no una regla general extensible a todo lo impertinente, sin que el recurrente haya identificado comunicaciones concretas comprendidas en esas hipótesis; y el artículo 223 confirma la misma lógica, porque la calificación de impertinencia y la destrucción son actos posteriores al examen. Concluye que esas normas no prohíben el examen del material impertinente, sino que regulan sus consecuencias, y que el estándar que de ellas deriva quedó resguardado en la resolución impugnada, que circunscribió temporalmente la búsqueda y prohibió incorporar a la carpeta y divulgar la información ajena a los hechos, sin perjuicio del derecho del amparado a solicitar en su oportunidad la restitución, destrucción o exclusión de lo impertinente o de lo obtenido con infracción de garantías.

Por su parte, Francis Patricia Fell Franco, jueza titular del mismo tribunal, informó que la resolución de 19 de agosto de 2026 se fundó en las solicitudes previas del Ministerio Público, en las medidas intrusivas antes autorizadas y en los antecedentes reunidos en la investigación, que dan cuenta de graves irregularidades cometidas por SOSER S.A. en la ejecución de contratos de licitación pública de servicios de alimentación en establecimientos educacionales de la región de O'Higgins, tales como la sobredeclaración de raciones, la falsificación de certificados, la incorporación de información falsa en los registros de la JUNAEB, la entrega de beneficios indebidos a directivos de establecimientos y encargados del programa y la distribución de alimentos contaminados, y que, respecto del amparado, permitían presumir delitos de soborno, cohecho y tráfico de influencias en relación con funcionarios públicos para favorecer a esa empresa, a lo menos desde el año 2018. Indica que la resolución se sustentó en informes de la Unidad de Análisis Financiero, documentación bancaria, transcripciones de audios, conversaciones de WhatsApp, comprobantes de transferencias y declaraciones, y en los resultados de las diligencias intrusivas autorizadas en julio de 2026, y que, conforme a los artículos 181, 187, 205, 209 y 217 del Código Procesal Penal, estimó la



diligencia necesaria, útil y proporcional. Añade que el levantamiento del secreto bancario se limitó al período que comienza en 2018 porque desde entonces la empresa habría desplegado las maniobras investigadas, y que los antecedentes forman parte de una investigación respecto de la cual el Ministerio Público decretó reserva el 24 de julio de 2026 conforme al artículo 31 de la Ley N° 19.913. Acompañó copia de la resolución.

Tercero: Que, en estrados, el Ministerio Público no informó el estado en que se encuentra la extracción del contenido de los dispositivos, si ella se completó o está pendiente, si se elabora un informe con su resultado ni la forma en que se conduce o conducirá la búsqueda de la información pertinente.

Cuarto: Que la acción constitucional de amparo, consagrada en el artículo 21 de la Constitución Política de la República, constituye un mecanismo de tutela de urgencia cuyo propósito es que la magistratura adopte de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado, frente a toda privación, perturbación o amenaza a su derecho a la libertad personal y seguridad individual que provenga de un acto u omisión contrarios a la Carta Fundamental o a las leyes.

Quinto: Que, como se advierte, el recurrente impugna la resolución que el Cuarto Juzgado de Garantía de Santiago dictó el 19 de agosto de 2026 en la causa RIT O-6719-2026, en cuanto autorizó el acceso a la totalidad de la información contenida en los dispositivos que le fueron incautados, y la de 26 de agosto de 2026, que rechazó delimitar ese acceso mediante criterios de pertinencia, lo que, a su juicio, amenaza y perturba su libertad personal y seguridad individual en relación con la vida privada y la inviolabilidad de las comunicaciones. Las juezas que informaron no niegan los hechos, sino que justifican sus decisiones en la ley y en los resguardos adoptados, que estiman suficientes. La cuestión a resolver consiste, entonces, en determinar si el tribunal, al autorizar la revisión de los dispositivos y al pronunciarse sobre la cautela pedida, satisfizo los deberes que la Constitución y el Código Procesal Penal le imponen respecto de una diligencia que la propia jueza que resolvió la cautela reconoció como lesiva de la privacidad del amparado y de terceros, o si, por el contrario, dejó la ejecución de esa diligencia sin el control que aquéllos exigen.



Sexto: Que, antes de entrar al fondo, conviene dejar sentado que la procedencia de esta acción ya fue resuelta. La Primera Sala de esta Corte la declaró inadmisibile el 8 de septiembre de 2026, por estimar que los hechos invocados se vinculan con materias que no se enmarcan en las hipótesis que resguarda el artículo 21 de la Constitución; apelada esa resolución, la Corte Suprema la revocó el 21 de septiembre de 2026, en los autos Rol N° 50.431-2026, por considerar que la situación descrita en el recurso sí puede constituir uno de los supuestos previstos en ese precepto, de cuyo mérito debe decidirse al conocer el fondo, y dispuso que una sala no inhabilitada diera al amparo la tramitación correspondiente “a fin de pronunciarse derechamente sobre el amparo deducido”.

Esa decisión se aviene con la doctrina que el máximo tribunal ha sostenido en casos semejantes, según la cual la libertad personal y la seguridad individual pueden verse amenazadas no sólo por vía principal, sino también de modo consecuencial, esto es, “con ocasión de la ejecución de un acto lesivo de uno o más derechos distintos”, y en ambos supuestos el amparo es el mecanismo idóneo para dejar sin efecto lo que ilegítimamente ponga en riesgo su ejercicio, pues reducir la acción a las afectaciones directas “importaría una injustificada restricción al derecho de accionar en procura de acceder a una tutela judicial efectiva” (SCS rol 12.292-2025, 28 de abril de 2025; en el mismo sentido, SCS rol 16.420-2025, 22 de mayo de 2025).

Por consiguiente, no corresponde a esta Sala volver sobre la admisibilidad y debe pronunciarse derechamente sobre la infracción denunciada.

Séptimo: Que los hechos relevantes no están discutidos. El 19 de agosto de 2026, en la investigación reservada que se sigue por delitos previstos en la Ley N° 20.393, fraude al fisco, fraude informático, delitos contra la salud pública, falsificación de instrumento privado, cohecho y lavado de activos, la jueza Francis Fell Franco, del Cuarto Juzgado de Garantía de Santiago, autorizó por diez días la entrada y registro de diversos domicilios y la incautación de teléfonos celulares, computadores y demás dispositivos de almacenamiento digital de titularidad de las personas que individualizó, entre ellas el amparado, a quien identificó como ex presidente de la asociación gremial Nutre Chile, “que pudieran dar cuenta



de reuniones, intercambios de información y otras formas de comunicación relacionadas a los hechos investigados”, y autorizó al persecutor y a la policía “el acceso, revisión, extracción y análisis de la información contenida en los dispositivos electrónicos incautados”, comprensiva de sus memorias internas y externas, de la tarjeta SIM, de las imágenes, videos, audios y de todo dato y registro almacenado en ellos, “así como en sus aplicaciones, redes sociales, correos electrónicos y nubes de almacenamiento a las que se halle vinculado el dispositivo”, sin acotar el período ni las materias de interés. Es la resolución a la que el informe de la jueza Guerrero González y la resolución de 26 de agosto se refieren como de 18 de agosto. El 20 de agosto se incautaron en el domicilio del amparado, según expone el recurso sin que los informes lo controviertan, su teléfono celular, el computador de su casa, un iPad y el computador de su oficina; por escrito de 25 de agosto su defensa pidió la cautela de sus garantías, que se vio en la audiencia del día siguiente junto con las promovidas por otros tres imputados; y en ella la jueza recurrida, Daniela Guerrero González, al resolverla, acotó temporalmente la búsqueda, prohibió entregar e incorporar a la carpeta lo ajeno a los hechos y remitió a dos instructivos internos del Ministerio Público, pero declinó fijar cualquier otro límite a la ejecución de la extracción, con la advertencia de que el persecutor accederá a información impertinente y privada. Lo que se examina, por ende, no es la legalidad de la incautación, que el recurrente no impugna, ni la procedencia misma del acceso al contenido de los dispositivos, que tampoco pretende impedir, sino la suficiencia de los términos en que el tribunal autorizó esa revisión y dejó que se ejecute, además de la fundamentación de la resolución que la dispuso.

Octavo: Que la respuesta exige partir de lo que hoy es un teléfono inteligente. Ningún otro objeto concentra tanta información sobre una persona. Acompaña a su dueño a toda hora; por él transitan sus conversaciones, sus fotografías, sus pagos y sus cuentas bancarias, su trabajo y la administración de su casa, y en su memoria se superponen, sin separación posible, la vida laboral, la doméstica y la afectiva. Tampoco admite, a diferencia del domicilio, un acotamiento espacial, pues en una casa puede registrarse una habitación y dejar cerradas las demás, mientras que quien accede a un teléfono accede a todo lo que contiene. La Corte



Suprema de los Estados Unidos lo describió en *Riley v. California*. Estos aparatos, dijo, son en realidad minicomputadores que reúnen en un solo lugar distintas clases de información, cuya combinación revela mucho más que cualquiera de ellas por separado; la suma de la vida privada de una persona puede reconstruirse a partir de un millar de fotografías fechadas y localizadas; la mayoría de sus dueños lleva consigo “un registro digital de casi todos los aspectos de sus vidas”; y un registro del teléfono “expondría típicamente al gobierno mucho más que el registro más exhaustivo de una casa” (*Riley v. California*, 573 U.S. 373, 393-397 y 403, 2014).

La misma idea llevó al Tribunal Constitucional Federal alemán a reconocer un derecho fundamental autónomo a la confidencialidad e integridad de los sistemas informáticos, comprensivo de los teléfonos móviles con múltiples funciones, al constatar que el acceso estatal a sistemas que contienen datos personales en tal cantidad y variedad permite reconstruir aspectos esenciales de la vida de una persona e incluso elaborar un perfil completo de su personalidad, y que ese riesgo existe ya en medidas de acceso aislado, como la incautación o copia de los soportes de almacenamiento, cuyos registros pueden incluir la correspondencia privada y profesional y anotaciones de carácter íntimo (BVerfG, sentencia de 27 de febrero de 2008, 1 BvR 370/07 y 1 BvR 595/07, BVerfGE 120, 274). El mismo tribunal advirtió que la gravedad de la injerencia aumenta cuando los datos revelan las comunicaciones del afectado con terceros, ya que la medida alcanza indiscriminadamente a esos interlocutores, respecto de los cuales no concurren los presupuestos que la justifican (*ibídem*).

Lo dicho vale, con igual o mayor razón, para los computadores, el iPad y demás dispositivos de almacenamiento masivo de información incautados al amparado, que contienen datos de la misma naturaleza y se examinan del mismo modo, de manera que los razonamientos de esta sentencia les son aplicables con las adaptaciones que su distinta configuración exija. Si el análisis se centra en el teléfono es porque en él concurren con mayor intensidad las características descritas.

Noveno: Que a esa constatación se suma la forma en que la diligencia se ejecuta. La revisión de un teléfono incautado no consiste en abrir una carpeta determinada, sino en obtener, mediante herramientas forenses, una copia íntegra de su contenido, la llamada copia espejo, sobre



la cual se practica después la búsqueda de lo pertinente. Al extraer, la técnica no distingue lo útil de lo que no lo es; se copia todo, desde los registros de las aplicaciones de mensajería y de correo hasta las fotografías, incluida la información personal, íntima y familiar del titular, y sólo con posterioridad se determina qué sirve a la investigación. Desde el punto de vista jurídico, generar esa copia equivale a apoderarse de todos los datos aunque el aparato se devuelva, porque el funcionario que la obtiene no sabe qué contenido ha copiado, sino sólo que ha tomado una copia de cuanto había en el dispositivo (Kerr, O. S., “Fourth Amendment Seizures of Computer Data”, en Yale Law Journal, vol. 119, 2010, pp. 709 y 717).

Por eso la lesión no se atenúa por la circunstancia de que el persecutor, una vez en posesión del acervo completo, seleccione después lo que quiere examinar, que es el supuesto del que parte la resolución recurrida cuando remite la protección a la exclusión probatoria posterior. La injerencia se consuma con la copia, no con el uso; desde ese momento el Estado dispone de toda la información y el afectado depende de la buena disposición del órgano que la tiene. La Corte Suprema estadounidense lo advirtió recientemente a propósito de los registros de localización que un servicio conserva de sus usuarios, al sostener que el alcance de la invasión “no se hace menor porque el gobierno, con el beneficio de la retrospectiva, pueda señalar exactamente qué pocas horas de desplazamientos quiere revisar” (Chatrie v. United States, No. 25-112, sentencia de 29 de junio de 2026, slip op. p. 21). En términos análogos, el Tribunal Europeo de Derechos Humanos ha subrayado que la separación de lo protegido y lo que no lo está adquiere especial relevancia cuando la incautación recae sobre grandes volúmenes de datos digitales o se practica mediante una copia espejo, y que resulta esencial impedir todo acceso no autorizado ni registrado a esos datos desde su incautación hasta su devolución o destrucción (TEDH, Sărgava c. Estonia, N° 698/19, 16 de noviembre de 2021). De ahí que el control no pueda diferirse al momento en que el persecutor decida usar la información, sino que deba recaer sobre la conservación misma de la copia, que es donde reside la afectación.

En el caso, la resolución recurrida da cuenta de esa realidad. La jueza dejó constancia de que “no es posible una exclusión ex ante de parte de la



información contenida en los dispositivos” y de que “no cabe duda de que el persecutor tendrá acceso a información que será impertinente y privada”. La afectación que aquí se examina no es, entonces, hipotética ni discutida; está reconocida en el acto impugnado y se extiende a terceros que no son imputados, como los familiares cuyas fotografías y mensajes alberga el aparato o las personas que se comunicaron con el amparado, cuya privacidad quedará expuesta sin que a su respecto concorra sospecha alguna.

A ello se agregan dos circunstancias propias de este caso. La primera es la condición de abogado del amparado, que el recurso invoca. Sus dispositivos no contienen sólo información suya; contienen la que sus clientes le confiaron en asuntos ajenos a esta investigación, cubierta por el deber de secreto que el artículo 303 del Código Procesal Penal reconoce y que pertenece a esos terceros y no al abogado. La jueza recurrida reconoció que indagar en esas comunicaciones no es parte de la investigación. Se trata, pues, de información que ni el persecutor ni terceros debieran llegar a conocer, y que por lo mismo debe quedar excluida de la búsqueda y eliminada de la copia obtenida o que se esté obteniendo, como se dispondrá. El Tribunal Europeo de Derechos Humanos ha exigido garantías procedimentales específicas cuando el material incautado o copiado es el de un abogado, incluso cuando es él mismo el sospechoso, porque lo protegido es la confianza de sus clientes y la posición que la abogacía ocupa en la administración de justicia, y ha reprochado que la orden de registro se limite a señalar que los investigadores accederán sólo a los datos relevantes, sin prever resguardo concreto alguno para el material amparado por el secreto (*Särgava c. Estonia*; *Nezirić c. Bosnia y Herzegovina*).

La segunda es que, hasta ahora, ninguna otra limitación se ha fijado. Como se dejó constancia, en estrados el Ministerio Público no informó el estado de la extracción, si ésta se completó o está pendiente, si se elabora un informe con su resultado ni cómo se conduce la búsqueda dentro de la copia; y la resolución de 19 de agosto de 2026 autorizó el acceso a todo el contenido de los dispositivos y de los servicios vinculados a ellos sin acotar materias, personas ni período. El único patrón que hoy delimita el examen es el temporal que la jueza recurrida impuso el 26 de agosto. Todo lo



demás, esto es, qué se busca, con qué criterios, quiénes acceden y qué ocurre con lo que no interesa, queda librado al arbitrio del órgano que ejecuta la diligencia.

Décimo: Que la intromisión no se agota en la memoria del aparato. El teléfono es, además, la llave de acceso a los servicios que su titular mantiene con la sesión abierta, esto es, cuentas de correo, redes sociales de acceso restringido, mensajería sincronizada y repositorios de almacenamiento en la nube, cuyos contenidos no residen en el dispositivo sino en servidores remotos, con frecuencia situados fuera del país, y a los que se llega con sólo pulsar la pantalla. Quien examina un teléfono desbloqueado puede alcanzar por esa vía información que nunca estuvo en poder de la policía, que el titular considera suya aunque la custodie un tercero y que en muchos casos pertenece también a otras personas, como ocurre con los grupos de mensajería, los perfiles cerrados de una red social o las carpetas compartidas. La Corte Suprema de los Estados Unidos advirtió en *Riley* que los datos que el usuario ve en su teléfono pueden no estar almacenados en él, que los agentes que revisan el aparato no sabrán normalmente si lo que miran estaba en el dispositivo o proviene de la nube, y que extender a esos archivos el registro del teléfono sería como encontrar una llave en el bolsillo de un sospechoso y sostener que ella autoriza a abrir y registrar una casa (*Riley v. California*, 573 U.S. 373, 397-398); y en *Chatrie* agregó que los registros que un servicio guarda en sus servidores se asemejan a los correos, documentos, fotografías o calendarios que el usuario razonablemente considera propios aunque estén alojados en servidores ajenos (*Chatrie v. United States*, slip op. p. 18). El Tribunal Constitucional Federal alemán, por su parte, incluyó expresamente en el ámbito del derecho a la confidencialidad e integridad de los sistemas informáticos los datos a los que el sistema da acceso en virtud de sus conexiones de red (BVerfG, sentencia de 27 de febrero de 2008).

Entre nosotros ese salto no es de cantidad sino de naturaleza. El acceso remoto a un dispositivo, computador o sistema informático mediante programas computacionales, contraseñas, códigos de seguridad o de acceso es una diligencia distinta, que el artículo 225 bis del Código Procesal Penal somete a petición fundada del Ministerio Público, a la existencia de fundadas sospechas basadas en hechos determinados y a una autorización



judicial específica, sujeta a un plazo máximo y a los requisitos de contenido que detalla el artículo 225 ter. Servirse de la sesión abierta en el teléfono incautado para ingresar a esos repositorios produce el mismo efecto que el registro remoto, con la diferencia de que se obtiene sin la resolución fundada que la ley exige para él; por eso no puede entenderse comprendido en la autorización para revisar el contenido del aparato y requiere una autorización expresa, que precise el servicio, la cuenta y el alcance del acceso. La Ley de Enjuiciamiento Criminal española lo resuelve en esos términos, al exigir autorización judicial para ampliar el registro desde el dispositivo incautado a los datos almacenados en otro sistema informático accesible desde él, salvo que la autorización inicial ya la comprenda, según su artículo 588 sexies c, apartado 3. En este caso, la resolución de 19 de agosto de 2026 extendió la autorización, en términos genéricos, a las aplicaciones, redes sociales, correos electrónicos y nubes de almacenamiento a las que se halle vinculado el dispositivo, sin individualizar servicios ni cuentas, sin acotar el período y sin las especificaciones que el artículo 225 ter exige para el registro remoto. Esa autorización es una de las impugnadas por esta vía, y su ejecución queda comprendida en el problema que aquí se resuelve, pues el acceso a esos repositorios multiplica el volumen de información privada, del amparado y de terceros, que el persecutor obtendrá. De ahí que las medidas de control que se dispondrán deban alcanzarlo, y que el Ministerio Público deba informar al tribunal a qué servicios y cuentas ha accedido o accederá por esa vía, para que el juez de garantía delimite ese acceso con arreglo a los artículos 225 bis y 225 ter.

Undécimo: Que la lesión así descrita no proviene de la ley, que nada dice sobre la revisión del teléfono incautado, sino de la resolución judicial que autoriza la diligencia y fija, o deja de fijar, sus términos. El artículo 9° del Código Procesal Penal somete a autorización judicial previa toda actuación del procedimiento que prive al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o los restrinja o perturbe, y el inciso segundo del artículo 5° ordena interpretar restrictivamente las disposiciones que autorizan la restricción de la libertad o de otros derechos del imputado. Si la ley confía al juez esa autorización, es porque espera de él algo más que un permiso; espera que pondere la intensidad de la injerencia frente al interés de la persecución y que la limite a lo que ese interés requiere. El



principio de proporcionalidad, con sus exigencias de idoneidad, necesidad y proporcionalidad en sentido estricto, es el método con que esa ponderación se realiza, y la doctrina nacional ha sostenido que el juez de garantía debe practicar ese test antes de decretar cualquier medida restrictiva de derechos fundamentales, comprobando que la diligencia sea adecuada al fin que se pretende, eligiendo entre las medidas idóneas la menos lesiva y verificando que las ventajas de la autorización guarden correspondencia con la vulneración que causa (Núñez Ojeda, R., Beltrán Calfurrapa, R. y Santander Akkrass, N., “Los hallazgos casuales en las diligencias de incautación e intervención de las comunicaciones digitales en Chile. Algunos problemas”, en *Política Criminal*, vol. 14, N° 28, 2019, pp. 159-160 y 180).

La Corte Suprema ha situado esa exigencia en el centro del control de las diligencias intrusivas, al declarar que el tribunal está obligado a requerir del persecutor las precisiones necesarias para despejar cualquier situación incierta, “principalmente para satisfacer correctamente el estándar de proporcionalidad que conlleva acceder a una diligencia invasiva de derechos fundamentales” (SCS rol 12.292-2025, 28 de abril de 2025). Trasladado ese estándar a la revisión de un teléfono, el juicio de necesidad impone al juez adoptar las medidas que reduzcan la afectación de la privacidad al mínimo compatible con el éxito de la investigación, y ello con mayor razón cuando la injerencia alcanza a terceros ajenos al proceso, que no han sido oídos ni pueden defenderse. Una autorización que reconoce que el persecutor accederá a información impertinente y privada y, en el mismo acto, renuncia a fijar cómo se acotará ese acceso y qué ocurrirá con lo excedente, no supera ese juicio.

Duodécimo: Que la intensidad de esta injerencia es, cuando menos, equivalente a la de las medidas que el Código sí regula con detalle. La interceptación de comunicaciones capta lo que se dice mientras se dice; el registro remoto de equipos informáticos aprehende el contenido de un sistema sin conocimiento del usuario; la extracción del teléfono incautado toma de una vez todo lo que se dijo, se escribió, se fotografió y se guardó durante años. Para las dos primeras el legislador exige fundadas sospechas basadas en hechos determinados. Sujeta la interceptación a delitos con pena de crimen y a que la investigación la haga imprescindible, y ordena que la resolución individualice al afectado, singularice los medios a



intervenir y señale al funcionario encargado, la forma, el alcance y la duración de la medida, que no puede exceder de sesenta días prorrogables sólo previo examen de la subsistencia de sus requisitos, como dispone el artículo 222; y limita el registro remoto a un plazo máximo de treinta días, prorrogable bajo la misma condición, conforme al artículo 225 bis. El artículo 225 ter, a su vez, exige que la resolución que autoriza el acceso remoto especifique los dispositivos objeto de la medida, “el alcance de la medida, la forma en la que se procederá al acceso y aprehensión de contenidos relevantes para la causa”, los agentes autorizados, la autorización para realizar y conservar copias, las medidas técnicas de preservación y “la duración precisa de la medida”. Y, cumplida la interceptación, el inciso cuarto del artículo 223 manda entregar a los afectados las comunicaciones impertinentes o irrelevantes y ordena que el Ministerio Público destruya toda transcripción o copia de ellas.

La Corte Suprema ha recordado que, por ser excepcionales las medidas que afectan la intimidad, la vida privada y la inviolabilidad de las comunicaciones, “el legislador exige un alto estándar de exigencias que deben cumplirse tanto por la fiscalía -para solicitarlas- como de motivación por el juez al dictar la resolución que las dispone” (SCS rol 18.430-2025, 3 de junio de 2025). No sería coherente que la diligencia más invasiva de todas, la que abarca a la vez las comunicaciones pasadas, las imágenes, los documentos, los desplazamientos y las relaciones del titular con terceros, quedara sometida a exigencias menores que la interceptación o el registro remoto por el solo hecho de que el Código, promulgado en el año 2000, cuando los teléfonos móviles no tenían las capacidades actuales, no la menciona, silencio que las reformas posteriores no han llenado, ni siquiera la Ley N° 21.577, que reguló el registro remoto de equipos informáticos, a diferencia de lo ocurrido en España, donde desde 2015 la ley disciplina de modo específico el registro de los dispositivos de almacenamiento masivo de información. El principio de proporcionalidad conduce a lo contrario, pues obliga a exigir de la petición del persecutor y de la resolución que la acoge, al menos, el mismo nivel de fundamentación y de precisión que el legislador impone a aquéllas.

Ninguna objeción cabe oponer a que esas exigencias se extiendan por vía analógica a una diligencia que la ley no regula. La prohibición de



analogía del inciso segundo del artículo 5° del Código Procesal Penal, que el recurso también invoca, alcanza a las disposiciones que autorizan la restricción de la libertad o de otros derechos del imputado, no a las que la condicionan o limitan; trasladar a la revisión del teléfono incautado los resguardos previstos para el registro remoto opera en beneficio del afectado y responde al deber que el inciso segundo del artículo 5° de la Constitución impone a los órganos del Estado de respetar y promover los derechos esenciales que emanan de la naturaleza humana. Por lo demás, si el acceso clandestino a un sistema informático debe acotarse en su alcance, forma, agentes, copias y duración, no se advierte por qué habría de quedar exento de esos límites el acceso que, sin ser clandestino, es compulsivo e impuesto, pues en uno y otro caso falta la voluntad del usuario para el registro y revisión de sus datos, y ante un grado equivalente de afectación de la garantía corresponden resguardos equivalentes.

El derecho comparado confirma esta orientación. La Ley de Enjuiciamiento Criminal española somete las medidas de investigación tecnológica a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, declara que “la simple incautación” de un teléfono u otro dispositivo de almacenamiento masivo “no legitima el acceso a su contenido”, exige una motivación individualizada para autorizarlo y dispone que la resolución que lo permite “fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos”, según sus artículos 588 bis a) y 588 sexies a), b) y c). Allí donde el legislador ha regulado la materia, en suma, no ha admitido que el acceso al contenido de un teléfono siga automáticamente a su incautación ni que la orden pueda omitir el alcance del registro y el destino de las copias.

Décimo tercero: Que de lo anterior se sigue el contenido mínimo que debe tener la resolución que autoriza la extracción y revisión de un teléfono. No basta con permitir el “peritaje” o el “vaciado” del aparato, porque sin determinación del objeto no hay modo de saber después qué fue búsqueda y qué fue hallazgo. El artículo 36 del Código Procesal Penal obliga a expresar “sucintamente, pero con precisión, los motivos de hecho y de derecho” de la decisión, y la Corte Suprema ha declarado que ese mandato integra las garantías mínimas del debido proceso y no se satisface con la mera relación de los antecedentes o de las solicitudes de los intervinientes



(SCS rol 14.900-2024, 9 de mayo de 2024; SCS rol 12.292-2025, 28 de abril de 2025). Aplicado a esta diligencia, el deber de fundamentación exige que el juez requiera del Ministerio Público, y consigne en su resolución, cuál es la información que se busca, determinada por los hechos investigados, las personas o cuentas con las que se pretende establecer comunicación, la época a que se refiere y las categorías de contenido pertinentes, así como la manera en que, obtenida la copia íntegra, se identificará lo útil y el plazo dentro del cual lo restante será eliminado de esa copia. Si el persecutor sostiene que alguna de esas determinaciones es técnicamente imposible, a él corresponde justificarlo ante el juez, y no al afectado demostrar lo contrario.

La proposición de esos criterios corresponde al Ministerio Público y no al juez. Definir los descriptores de una búsqueda dirigida, sean palabras clave, interlocutores, cuentas, tipos de archivo o rangos de fechas, es una función investigativa que exige el dominio de los antecedentes reunidos, de la hipótesis que se indaga y de las técnicas forenses e informáticas con que se examina una copia, conocimientos que el tribunal no posee y que el artículo 83 de la Constitución radica en el persecutor. Lo que el juez puede y debe exigir es que esa propuesta exista antes de que la copia se examine, que quede registrada, que sea puesta en su conocimiento y que sea razonable, pues sólo así el control posterior contará con un punto de referencia contra el cual medir lo que se hizo. Este último requisito no es menor. Unos criterios tan amplios que capturen la mayor parte del contenido, como sería buscar por términos de uso corriente o por interlocutores indeterminados, equivalen a no tener criterios, y bajo su apariencia la revisión termina por abarcarlo todo, de modo que cuanto aparezca podrá presentarse después como un hallazgo casual que en realidad estaba preconstituido por la amplitud de la búsqueda; frente a una propuesta de esa índole, el juez debe exigir su acotamiento antes de que el examen comience. Así lo entendió la Corte de Apelaciones de Valparaíso en un amparo reciente, deducido por una imputada contra la negativa del juez de garantía a limitar el examen de los dispositivos que le fueron incautados, al ordenar que los descriptores de búsqueda fueran informados al juzgado de garantía (SCA de Valparaíso rol 3810-2026, 1 de septiembre



de 2026, confirmada por SCS rol 49.866-2026, 24 de septiembre de 2026, con declaración sobre las medidas a cargo del Ministerio Público).

Esos criterios han de aplicarse, ante todo, a las aplicaciones de mensajería, al correo electrónico y a las redes sociales, que son hoy el principal depósito de las comunicaciones de una persona y, previsiblemente, el objeto central del examen, y no sólo a los archivos que el aparato guarda en sus carpetas. Sus registros forman parte del contenido extraído, sea que estén almacenados en el dispositivo o que la aplicación los sincronice desde servidores remotos a través de la sesión abierta, según se dijo en el considerando décimo, y quedan sujetos a las mismas limitaciones. Respecto de ellos, la delimitación por cuenta, interlocutor y período es la que permite que el persecutor lea las conversaciones y los correos intercambiados con las personas y en la época que interesan a la investigación, y no la totalidad de los intercambios del amparado con quienes nada tienen que ver con ella, mientras que las palabras clave y las categorías de contenido cumplen esa función respecto de las conversaciones de grupo y de las casillas con numerosos remitentes. Las herramientas de análisis forense permiten filtrar los registros extraídos por contacto, cuenta, fecha y término de búsqueda, de modo que la limitación no es impracticable y, si el persecutor sostuviere lo contrario en algún caso, deberá justificarlo ante el juez.

Distinto es el caso de las fotografías, los videos y los audios. Su contenido no está expresado en texto, de modo que las palabras clave no permiten seleccionarlos; lo que sí permite acotar el universo son los datos asociados a cada archivo, esto es, la fecha en que se creó o recibió, el lugar en que se captó y la conversación, correo o cuenta de la que proviene. Por eso, respecto de estos archivos, la limitación opera a través del período y de la procedencia, y dentro del conjunto así delimitado no hay otro modo de saber si son pertinentes que verlos u oírlos, revisión directa que, por lo mismo, importa una intromisión mayor y exige, como compensación, que la practiquen sólo los funcionarios individualizados, que no se generen copias adicionales, que se deje constancia de los archivos que se conservan y que los restantes, entre ellos los de carácter familiar, conyugal, íntimo o de salud y los relativos a su función de abogado en asuntos ajenos a los hechos, cuya exclusión el recurso solicita, se eliminan con el excedente. Pretender



que el persecutor identifique lo útil sin mirar sería tan ilusorio como permitirle mirar sin límite y sin registro.

La experiencia europea muestra el costo de omitir esas determinaciones. En *Särgava c. Estonia*, el Tribunal Europeo de Derechos Humanos constató que la orden de registro no previó resguardo alguno para el material protegido, que la búsqueda por palabras clave sobre la copia del teléfono y del computador de un abogado no derivaba de la ley ni de la orden, sino de una decisión de los propios investigadores, quienes eligieron términos tan amplios como “ejercicio financiero” o “línea de crédito”, y que el derecho interno no ofrecía mecanismo alguno para que el material disputado no llegara a los investigadores antes de que un tribunal lo analizara y, de ser necesario, ordenara su devolución o destrucción; por ello declaró violado el artículo 8 del Convenio. Y en *Nezirić c. Bosnia y Herzegovina* reiteró que copiar íntegramente el teléfono de un abogado y filtrar la copia con los números de los coimputados, sin que esa limitación proviniera de la ley ni estuviera sujeta a supervisión judicial, carece de las garantías procedimentales que exige el Convenio (TEDH, *Nezirić c. Bosnia y Herzegovina*, N° 4088/21, 5 de noviembre de 2024).

Décimo cuarto: Que, si el persecutor no ofrece esa delimitación, el juez debe exigirla y, en su defecto, establecerla. La cautela de garantías del artículo 10 del Código Procesal Penal lo faculta para adoptar, “de oficio o a petición de parte, las medidas necesarias” para permitir el ejercicio de los derechos del imputado, y el artículo 14 letra a) del Código Orgánico de Tribunales le encomienda “asegurar los derechos del imputado y demás intervinientes en el proceso penal”. En una diligencia que necesariamente pasa por la copia total del dispositivo, esas medidas consisten, cuando menos, en fijar un plazo para culminar la extracción y la identificación del contenido útil, en ordenar la eliminación del resto de la copia con certificación de haberse practicado y en resolver sobre la devolución del aparato o, si su conservación es necesaria, sobre su custodia. Nada de ello es ajeno a nuestro sistema. El deber de destruir las copias de lo impertinente ya está en el inciso cuarto del artículo 223 para las interceptaciones, y no se advierte razón para excluir de él a un registro que compromete la privacidad con mayor intensidad; la fijación de plazos y de una duración precisa está en los artículos 222 y 225 ter; y la custodia de lo



incautado, con acceso de los intervinientes autorizado por el fiscal o, en su caso, por el juez de garantía, en el artículo 188.

El Tribunal Constitucional Federal alemán llegó a la misma solución cuando admitió que, en el acceso a sistemas informáticos, es prácticamente inevitable obtener información antes de poder determinar si pertenece al núcleo de la vida privada; en tal caso, dijo, la protección debe asegurarse en la fase de análisis, mediante un procedimiento que examine los datos recogidos y disponga que los que pertenezcan a ese núcleo se eliminen sin dilación y no puedan utilizarse ni transmitirse (BVerfG, sentencia de 27 de febrero de 2008). En el ámbito del Convenio Europeo, el control judicial posterior fue la garantía decisiva en *Sérvulo & Asociados c. Portugal*, donde no se declaró violación porque el juez de instrucción revisó lo incautado en un estudio de abogados y ordenó destruir cerca de 850 archivos que contenían información personal, cubierta por el secreto profesional o relativa a personas no investigadas (TEDH, *Sérvulo & Asociados - Sociedade de Advogados, RL y otros c. Portugal*, N° 27013/10, 3 de septiembre de 2015). Y entre nosotros, el fallo de la Corte de Apelaciones de Valparaíso ya citado dispuso, además de la comunicación de los descriptors de búsqueda, que el Ministerio Público informara al tribunal los funcionarios con acceso a los dispositivos, dejara fuera del análisis lo impertinente y eliminara toda la información extraída fuera de esos límites, informando los protocolos seguidos y las personas encargadas. Al confirmarlo, la Corte Suprema declaró que los dispositivos incautados y su custodia deben quedar únicamente a cargo del fiscal responsable de la investigación, que el Ministerio Público debe informar al juez de garantía el nombre de los funcionarios que tendrán acceso a ellos, que no puede utilizarse información anterior a la época que fijó, que debe quedar fuera de análisis toda la información que carezca de pertinencia con los hechos que justificaron la incautación, a excepción de los hallazgos que puedan revestir caracteres de otros ilícitos, y que toda la información extraída fuera de esos límites, y de la que se hubieren hecho copias sin interés criminalístico, debe ser eliminada, informando al tribunal los protocolos seguidos y las personas encargadas de su ejecución. Recordó, asimismo, que el Código no sólo regula los casos y formas de la interceptación, sino también, en el artículo 223, el destino de la información



obtenida, como lo hace el inciso final del artículo 218 para la correspondencia.

Décimo quinto: Que la determinación del objeto tiene otra consecuencia, referida a los hallazgos que se produzcan durante la revisión. El artículo 215 del Código Procesal Penal permite incautar los objetos o documentos que, durante la práctica de un registro, hagan sospechar la existencia de un hecho punible distinto. Esa regla se concibió para la entrada y registro en lugares cerrados, donde las divisiones físicas permiten deslindar lo autorizado de lo que no lo está. En el interior de un teléfono no hay habitaciones ni cajones que separen unos contenidos de otros; todo está al alcance del mismo examen. Si bastara, entonces, con que un contenido apareciera durante la revisión para autorizar su uso, la orden que recae sobre un teléfono se convertiría en una orden sobre todo el teléfono, y la determinación de su objeto perdería todo sentido. La doctrina ha advertido que, conforme al principio de especialidad, no es admisible una incautación destinada a descubrir, sin la adecuada precisión, actos delictivos cualesquiera, lo que convertiría la orden en una autorización en blanco, y que admitir el hallazgo casual sin límites llevaría a que “cualquier incautación de un dispositivo informático se transforme en una búsqueda general, habilitada para capturar cualquier evidencia de cualquier delito” (Núñez Ojeda, R., Beltrán Calfurrapa, R. y Santander Akkrass, N., *ob. cit.*, pp. 173 y 180; en el mismo sentido, pp. 176-177).

De ahí que el persecutor no pueda servirse de la copia para revisar el teléfono en busca de otros delitos. Si la orden no fija límites a la revisión, todo lo que aparezca en la copia será, por definición, encontrado “casualmente”, y la excepción del hallazgo casual, pensada para lo que surge sin buscarlo, terminará por cubrir lo que la orden debía impedir, esto es, la revisión exploratoria de todo el contenido en busca de algún delito, sin saber cuál, que la doctrina y la jurisprudencia comparadas llaman investigación prospectiva. Con límites, en cambio, el hallazgo es casual sólo cuando se produce de manera inevitable en el curso de la ejecución legítima de la orden y dentro de ellos; cuando la revisión se extiende deliberadamente a contenidos que la orden no cubría, lo encontrado no es fruto del azar, sino de una desviación de la orden judicial que no puede aprovecharse. Es al Ministerio Público a quien corresponde acreditar que la



ejecución de la orden, respetado el principio de especialidad, conducía necesariamente a la información del delito distinto, porque es él quien conduce el examen, quien está en condiciones de registrar cómo se practicó y sobre quien pesa el deber de fundamentar sus actuaciones. Esta Corte ya advirtió, al conocer de una acción de protección referida a la transcripción de centenares de miles de páginas de mensajería extraídas de un teléfono, que la orden judicial sólo pudo referirse a las conversaciones relacionadas con el objeto de la investigación y que es deber del Ministerio Público cautelar, en su labor, los derechos constitucionales de los terceros ajenos a ella (SCA de Santiago rol 6423-2024, 28 de junio de 2024); y el voto de minoría de ese fallo, que estuvo por acoger la acción, precisó que el persecutor no puede, sin incurrir en ilegalidad, hurgar en esas transcripciones en una suerte de búsqueda de ilícitos ajenos al objetivo de la orden judicial, pues el orden correcto es el inverso, esto es, iniciar una investigación por un delito determinado y, según los datos que ella arroje, solicitar la autorización para develar los mensajes, sin que la autorización otorgada constituya “una especie de patente de corso” para buscar y rebuscar en ellas algún ilícito distinto del que inició la investigación. Cuando, en el curso de la revisión legítima, aparezca información sobre otro hecho punible, lo procedente será ponerla en conocimiento del juez de garantía y obtener de él la autorización para utilizarla, con el umbral de gravedad que el inciso final del artículo 223 fija para la información obtenida en una interceptación, analogía que se impone por la equivalente intensidad de ambas injerencias, en lugar de acudir a la más laxa del artículo 215, pensada para un continente físico.

Ese control se ejerce después de la revisión y tiene un objeto preciso. Corresponde al juez que autorizó la diligencia, aunque la investigación del nuevo delito llegue a radicarse ante otro tribunal, porque es él quien fijó los límites de la orden y recibió los criterios de búsqueda, de modo que sólo él está en condiciones de cotejar lo hecho con lo autorizado y de verificar que su orden no haya sido excedida bajo la apariencia de un hallazgo; así ocurre en las medidas intrusivas que la ley regula, en que el mismo juez que las autoriza examina cada vez la subsistencia de sus requisitos para prorrogarlas, y así lo dispone el inciso cuarto del artículo 220 cuando entrega al juez, a la vista de los objetos, la decisión sobre la legalidad de la



incautación. Dejar esa verificación para el tribunal de la causa nueva significaría que el Ministerio Público podría invocar siempre un hallazgo casual y diferir el control a un juez que sólo intervendría si esa otra investigación prospera, conservando entretanto la información privada y eludiendo los resguardos aquí descritos. Cuando el Ministerio Público invoque un hallazgo, deberá explicar ante el juez que autorizó la diligencia con qué descriptor, palabra clave, interlocutor o filtro llegó a la información de que se trata, y el tribunal apreciará si esa búsqueda era razonable en relación con el objeto autorizado y con los criterios comunicados, en cuyo caso el hallazgo será casual y podrá autorizar su uso, o si se trató de una revisión exploratoria que ninguno de esos criterios justificaba, o de criterios tan amplios que la revisión abarcó en los hechos todo el contenido, en cuyo caso la información se obtuvo fuera de los supuestos que la ley admite, no podrá utilizarse en esta ni en otra investigación y deberá eliminarse junto con el excedente de la copia. No se trata de anticipar el debate sobre exclusión de prueba de la audiencia de preparación del juicio oral, que conserva su ámbito respecto de lo que se ofrezca como evidencia en esta causa, sino de controlar la ejecución de una orden intrusiva, tarea que pertenece al juez que la dictó. Autorizado el uso, la investigación del hecho distinto seguirá su curso ante el tribunal que corresponda. El derecho comparado conoce, a título ilustrativo, exigencias semejantes, pues la Ley de Enjuiciamiento Criminal española sólo permite utilizar en otro proceso la información obtenida en una medida de investigación tecnológica dejando constancia de la solicitud inicial, de la resolución que la acordó y de sus prórrogas, y somete la continuación de la medida respecto del delito casualmente descubierto a un nuevo control judicial, según sus artículos 579 bis y 588 bis i.

Décimo sexto: Que las medidas descritas no suponen que el juez de garantía se entrometa en la investigación ni que determine qué información es útil para ella, decisión que el artículo 3° del Código Procesal Penal y el artículo 83 de la Constitución reservan al Ministerio Público. El juez no selecciona la prueba; fija las condiciones bajo las cuales una diligencia que él autorizó puede ejecutarse sin afectar más de lo necesario los derechos del imputado y de terceros, que es la función que el artículo 14 letra a) del Código Orgánico de Tribunales le asigna. No es extraño a nuestro sistema



que el juez oriente de ese modo la ejecución de una diligencia. El legislador, al regular el registro remoto de equipos informáticos, exige que la resolución que lo autoriza especifique “la forma en la que se procederá al acceso y aprehensión de contenidos relevantes para la causa”, según la letra b) del artículo 225 ter, forma que el fiscal propone en su solicitud y que el juez fija y controla, sin que nadie haya visto en ello una intromisión en la dirección de la investigación. La Corte Suprema ha destacado la importancia de establecer altos estándares de exigencia respecto de la actuación de los sujetos procesales en las primeras diligencias del procedimiento, “siendo una función esencial del Juez de Control adoptar las medidas necesarias que permitan la protección y el ejercicio de las garantías que la Constitución, las Leyes y los Tratados Internacionales otorgan a todas las personas” (SCS rol 14.900-2024, 9 de mayo de 2024). El juez que autoriza una intromisión no puede, por lo mismo, desentenderse de sus efectos. La Corte Suprema lo ha dicho al confirmar el fallo de la Corte de Valparaíso ya citado: no basta con que la judicatura haya autorizado al Ministerio Público para que la afectación del derecho sea legítima, pues “una comprensión tan acotada de la intervención judicial equivaldría a una delegación de sus facultades jurisdiccionales” y a una vulneración del mandato constitucional de reserva de ley para la afectación justificada y proporcional del derecho (SCS rol 49.866-2026, 24 de septiembre de 2026).

Tampoco altera esta conclusión la autonomía que el artículo 83 de la Constitución reconoce al persecutor, en cuyo resguardo la resolución recurrida calificó de intromisión indebida toda limitación previa del examen. Esa misma norma dispone que las actuaciones que priven al imputado o a terceros del ejercicio de los derechos que la Constitución asegura, o los restrinjan o perturben, requieren de aprobación judicial previa, de modo que la intervención del juez en la delimitación de tales actuaciones no es una injerencia en la dirección de la investigación, sino el presupuesto constitucional de su legitimidad. Dirigir la investigación es decidir qué se investiga y con qué diligencias; señalar los términos en que una de ellas puede afectar la privacidad de las personas es tarea del tribunal. Por eso la Corte de Apelaciones de Valparaíso pudo observar, en el precedente citado, que el equilibrio entre los derechos de la imputada y las prerrogativas del Ministerio Público exige protocolos preestablecidos y rigurosos en el



examen y traspaso de la información contenida en los dispositivos, y que su mayor especificación por la judicatura, “que es la primera llamada a asegurar el pleno respeto de las garantías de los intervinientes”, no debiera causar inquietud al persecutor.

Décimo séptimo: Que el silencio del Código Procesal Penal sobre el vaciado y revisión de teléfonos, computadores y otros equipos incautados no priva al juez de esas atribuciones ni deja la diligencia sin límites; significa sólo que éstos deben construirse desde los principios que gobiernan a todas las medidas intrusivas, esto es, la autorización judicial previa del artículo 9°, la interpretación restrictiva del artículo 5° y la fundamentación del artículo 36, y desde la facultad que el artículo 10 confiere al juez para adoptar de oficio las medidas necesarias en cautela de las garantías. El recurso extrae de ese silencio una conclusión distinta, esto es, que ninguna norma habilita el registro del contenido de un dispositivo incautado, pues el artículo 218 bis sólo regula la preservación provisoria de datos en poder de proveedores de servicios, y que el tribunal extendió por analogía una habilitación que la ley no contempla. No es así. La incautación de los objetos y documentos que puedan servir como medios de prueba está prevista en los artículos 187 y 217 del Código, y el examen de lo incautado es inherente a la finalidad probatoria que la justifica, tanto que el propio recurrente no pretende que se impida al Ministerio Público acceder al contenido de sus dispositivos. Lo que la ley no regula es la forma de ese examen, y ese vacío no se llena extendiendo la autorización, sino limitándola con las exigencias que rigen a las diligencias intrusivas reguladas, aplicadas, según se dijo en el considerando duodécimo, en beneficio del afectado y no en su contra. El Tribunal Europeo de Derechos Humanos, ante la ausencia de una regulación específica del acceso policial al contenido de un computador, ha exigido igualmente que el derecho interno, integrado por la jurisprudencia, imponga la autorización judicial previa y un control judicial efectivo, y ha declarado violado el Convenio cuando el examen íntegro de los archivos se practicó sin ella y sin urgencia que lo justificara (TEDH, Trabajo Rueda c. España, N° 32600/12, 30 de mayo de 2017).

Décimo octavo: Que el control descrito exige, además, una oportunidad para ejercerlo. La orden que autoriza la extracción debe señalar desde ya la audiencia en que se verificará su cumplimiento, en particular



para disponer la destrucción del excedente de la copia y resolver sobre la devolución o custodia del aparato, del mismo modo que la interceptación y el registro remoto tienen una duración precisa y una prórroga sujeta a nuevo examen judicial. No basta con remitir la cuestión a la audiencia de preparación del juicio oral, como hace la resolución recurrida. La exclusión probatoria sólo operaría si el persecutor decide usar la información, en un procedimiento que puede no llegar a esa etapa y que en nada resguarda a los terceros, que no son intervinientes y jamás sabrán que sus comunicaciones fueron revisadas; y, entretanto, ni el imputado ni esos terceros tienen por qué soportar, sin una justificación que la ley no ofrece, que un órgano del Estado conserve durante meses o años, en una copia sobre la que ningún tribunal ejerce control, información sobre sus vidas que no guarda relación con el delito investigado. La retención de esos datos es por sí misma una injerencia que se prolonga en el tiempo, y no un mero antecedente de la que se produciría al usarlos; por eso el inciso cuarto del artículo 223 no espera al juicio para ordenar la destrucción de las copias de lo impertinente, y por eso los tribunales citados en el considerando décimo cuarto sitúan la eliminación inmediatamente después del examen y cuentan la injerencia desde la incautación hasta la destrucción. Una investigación de la envergadura de la presente puede prolongarse largamente antes de que se formule acusación, si es que se formula, y durante todo ese lapso, sin las medidas que aquí se disponen, el contenido íntegro de los dispositivos permanecería a disposición del persecutor.

Décimo noveno: Que los instructivos del Ministerio Público a los que remite la resolución recurrida no bastan para conjurar la afectación descrita. El Oficio FN N° 983/2024 constituye, según sus propios términos, “normativa interna del Ministerio Público”; se aplica sólo a las causas complejas que el fiscal regional decida someter a él; confía al fiscal la evaluación inicial acerca de si la información es o no sensible y de interés investigativo; le permite considerar que toda la información de la carpeta es de interés investigativo, no sujeta a regla de protección; radica en él la decisión de anexar lo impertinente, que no se elimina sino que se guarda en custodia con un número único de evidencia, y prevé que, cuando surjan nuevas líneas de indagación, el mismo fiscal pueda estimar que lo anexado es relevante y, con autorización del fiscal regional, reincorporarlo a la



carpeta. El Oficio FN N° 363/2025, por su parte, ordena a los fiscales instruir a las policías que excluyan de los informes policiales la información de la vida privada penalmente irrelevante y, si el informe la incluye, pedir una audiencia para que tales antecedentes queden reservados. Ninguno de los dos contempla la eliminación del excedente de la copia forense, ni plazos, ni un control judicial en una oportunidad determinada; la información privada e impertinente queda, en todos los casos, en poder del persecutor y bajo su exclusiva apreciación.

La misma jueza recurrida reconoció que esos instructivos dejan a salvo sólo “varias de las aprehensiones” de los litigantes y se mostró dispuesta a complementar lo resuelto para limitar o aclarar su alcance, lo que confirma que la protección quedó incompleta. Los criterios internos de actuación son valiosos, pero no sustituyen la garantía judicial, porque la decisión sobre el alcance de una injerencia en derechos fundamentales no puede quedar entregada al órgano que la ejecuta y tiene interés en su resultado. En *Särgava c. Estonia* el Tribunal Europeo estimó insuficiente que el filtrado de la copia hubiera quedado enteramente en manos de las autoridades investigadoras, y en *Nežirić c. Bosnia y Herzegovina* no bastó que los investigadores hubieran actuado concienzudamente y tratado los datos como secreto oficial, porque la búsqueda selectiva no derivaba de la ley y se practicó sin supervisión judicial. La Corte Suprema estadounidense, en fin, frente a la propuesta del Gobierno de que las agencias desarrollaran protocolos para resolver los problemas del acceso a los datos del teléfono, observó que probablemente era una buena idea, pero que los fundadores no habían combatido una revolución para obtener el derecho a los protocolos de las agencias gubernamentales (*Riley v. California*, 573 U.S. 373, 398).

Vigésimo: Que no cabe acoger, en cambio, la pretensión de que los descriptores, palabras clave y rangos de búsqueda se fijen previamente oyendo a la defensa, ni la de que las personas cuyas comunicaciones interesan a la investigación se determinen con su intervención. En nuestro sistema la apreciación de qué información es útil para la investigación corresponde únicamente al Ministerio Público, que la dirige en forma exclusiva conforme a los artículos 83 de la Constitución y 3° del Código Procesal Penal y que, además, cuenta con los medios técnicos y la



capacidad de análisis para efectuarla. La proposición de los criterios de búsqueda es una función investigativa y su control pertenece al juez; hacer intervenir a la defensa en esa definición convertiría la ejecución de una diligencia de investigación en un debate contradictorio que nuestro sistema no contempla, y no es necesario para el resguardo que se persigue, pues la defensa conocerá esos criterios en la audiencia de control que se dispondrá y podrá entonces objetar la forma en que se practicó la búsqueda. Lo que el juez puede y debe hacer es fijar los límites de la búsqueda, recibir del persecutor los criterios con que la practicará, apreciar si son razonables y controlar después su cumplimiento, no ejecutarla ni sustituir al persecutor en la selección de la evidencia. Tampoco se trata, como temió la recurrida, de dejar la entrega de la información al arbitrio de la persona investigada, pues los criterios los propone el persecutor y los aprueba el juez, sin que el imputado intervenga en su definición. Ni hay motivo para encomendar el control de lo que aquí se dispone a un juez distinto de los que dictaron las resoluciones recurridas, como también se pide; esa tarea corresponde al Cuarto Juzgado de Garantía de Santiago, cualquiera sea el juez que lo sirva, pues es el tribunal que autorizó la diligencia y conoce de la investigación, y el haber resuelto la cautela en un sentido que esta sentencia corrige no es motivo para apartar a sus jueces del control de lo que ahora se ordena.

Vigésimo primero: Que, asimismo, no procede la exclusión previa y en bloque de las comunicaciones del amparado con su cónyuge, sus parientes y sus abogados y de las amparadas por el secreto profesional, en los términos en que el recurso la pide, ni el artículo 220 del Código Procesal Penal, en que la funda, ofrece la solución del caso. Esta norma impide incautar las comunicaciones entre el imputado y las personas que pueden abstenerse de declarar por parentesco, conforme al artículo 302, o por razón de secreto, conforme al artículo 303, así como las notas y documentos a que se extiende esa facultad, pero su inciso segundo dispone que esas limitaciones “sólo regirán” cuando tales objetos “se encontraren en poder de las personas a quienes la ley reconoce la facultad de no prestar declaración”, y las extiende a las oficinas o establecimientos de los profesionales del artículo 303. La norma protege, entonces, la confianza que el imputado deposita en su pariente, su abogado, su médico o su confesor,



y lo hace impidiendo que lo confiado se incaute en manos de estos últimos; su ámbito propio sería el teléfono, el dispositivo o los papeles del abogado defensor del amparado, en los que constaran las consultas o la asesoría de su defensa, y no el caso de autos, en que lo incautado son los dispositivos del imputado mismo, pues la norma no establece una prohibición general de incautar sus comunicaciones dondequiera que se encuentren. A ello se agrega que el inciso tercero excluye las limitaciones cuando las personas facultadas para no prestar testimonio fueren imputadas por el hecho investigado, de modo que, aun si los dispositivos del amparado se miraran como el archivo profesional de un abogado y sus clientes fueran los imputados cuya confianza se resguarda, la protección cedería igualmente, por revestir el propio abogado la calidad de imputado, como lo resolvió la recurrida. Ni el artículo 360 del Código de Procedimiento Civil ni el artículo 64 del Código de Ética Profesional, que el recurso también invoca, alteran esa conclusión, pues el primero sólo exime al abogado de declarar como testigo sobre los hechos que se le han comunicado confidencialmente con ocasión de su profesión, y el segundo, cualquiera sea el valor que se le reconozca, regula los deberes del abogado hacia sus clientes y no puede conferirle una inmunidad frente a la investigación de un delito que se le imputa, que sólo la ley podría establecer.

Descartado que el artículo 220 sea aplicable al caso de autos, y para mayor claridad de lo que se resolverá, conviene entonces distinguir tres situaciones.

La primera es la de las comunicaciones que el amparado, en cuanto imputado, haya mantenido con sus abogados defensores, en esta o en otras causas judiciales, para preparar y ejercer su defensa. Están protegidas, aunque no específicamente por el artículo 220, sino por el derecho a la defensa que aseguran el artículo 19 N° 3 de la Constitución y el artículo 8° del Código Procesal Penal, y por la misma razón que lleva al inciso tercero del artículo 222 a prohibir la interceptación de las comunicaciones entre el imputado y su abogado, salvo que el juez estime fundadamente que éste pudiere tener responsabilidad penal en los hechos investigados. Por eso, si los dispositivos las contienen, deben quedar excluidas de la búsqueda y eliminarse de la copia, aun cuando los criterios de búsqueda las alcancen, a



menos que el abogado de que se trate sea también imputado por los hechos investigados, circunstancia que no se ha planteado en esta causa.

La segunda es la de las comunicaciones con los clientes a quienes asistió como abogado en asuntos ajenos a los hechos investigados, y las que mantuvo con su cónyuge, sus parientes y demás personas ajenas a ellos. Su protección, como se dijo, no proviene del artículo 220 y, más allá del secreto profesional o del parentesco, que sólo alcanzarían a una parte de lo que los aparatos contienen, reside en la garantía que los numerales 4° y 5° del artículo 19 de la Constitución dispensan a toda comunicación y a toda forma de vida privada, del amparado y de esos terceros, respecto de información que, según la propia recurrida, no guarda relación con los hechos investigados. Ese criterio, la impertinencia de la información, cubre por igual las comunicaciones con clientes, familiares, amigos o cualquier otra persona, es el que subyace a lo dicho en el considerando noveno y justifica que se ordene excluirlas de la búsqueda y eliminarlas de la copia. No era necesario, por lo demás, para obtener ese resguardo, que el amparado identificara comunicaciones concretas, como echa de menos el informe, pues no podría hacerlo sin conocer el objeto preciso de una investigación que le está reservada, y la propia recurrida admitió que el persecutor accederá a información impertinente y privada.

La tercera es la de las comunicaciones con esas mismas personas que sí se relacionan con los delitos investigados. No cabe excluirlas de antemano en bloque, porque los criterios de búsqueda, determinados por los hechos, las personas y la época de interés, pueden conducir a intercambios que el amparado sostuvo con un cliente, un representado, su cónyuge o un pariente y que conciernen a esos hechos; si quedan comprendidas en esos criterios, y dado que el amparado es imputado, tales comunicaciones son pertinentes, y la facultad de abstenerse de declarar que los artículos 302 y 303 reconocen al pariente o al profesional no crea, sobre los registros que el imputado guarda en sus dispositivos, una zona inmune a la investigación que se sigue en su contra, de suerte que pueden ser examinadas, conservadas y utilizadas.

Por último, no cabe aplicar por analogía el mecanismo del inciso cuarto del artículo 220, que ante la duda sobre la procedencia de la incautación permite al juez ordenarla y examinar él mismo los objetos, sin



intervención previa del fiscal ni de la policía, para decidir sobre la legalidad de la medida y ordenar la devolución de lo protegido, como pide el recurso respecto de las comunicaciones de calificación dudosa. Ese examen recae sobre elementos objetivos, como si el tenedor es una persona exenta de declarar, si el documento es un diagnóstico médico o una nota tomada por el abogado sobre lo que su cliente le confió, y por eso puede confiarse al juez a la vista de los objetos; nada tiene en común con determinar si una conversación, una fotografía o un archivo son útiles para una investigación, juicio que exige conocer la hipótesis delictiva y los antecedentes reunidos y que pertenece al persecutor. En lo que la resolución recurrida acertó fue en señalar que indagar en las comunicaciones del amparado con sus clientes no es parte de la investigación, con lo que se hizo cargo del secreto profesional invocado; lo que faltó fue hacer efectivo ese resguardo con medidas concretas.

Vigésimo segundo: Que tampoco serán acogidas las peticiones dirigidas contra la resolución de 19 de agosto de 2026. El recurso le reprocha, en primer término, carecer de la fundamentación que exigen los artículos 9° y 36 del Código Procesal Penal, por remitirse al mérito de los antecedentes de la solicitud fiscal y a resoluciones anteriores que la defensa desconoce. La lectura de la resolución no confirma ese reproche. Ella individualiza los delitos investigados; describe los hechos que se indagan, esto es, las irregularidades atribuidas a SOSER S.A. en la ejecución de contratos de alimentación escolar en la región de O'Higgins y el soborno y cohecho de funcionarios públicos para obtener información reservada y la adjudicación de licitaciones; enuncia los antecedentes en que se apoya, a saber, informes de análisis financiero, documentación bancaria, transcripciones de audios, mensajería de WhatsApp, fotografías de conversaciones y de transferencias y declaraciones; da cuenta de los resultados de las diligencias intrusivas practicadas en julio de 2026; expone el mecanismo que esos antecedentes revelarían y las categorías de personas involucradas; y califica la diligencia de necesaria, útil y proporcional para determinar los hechos y la participación. Expresa, pues, sucintamente y con precisión, los motivos de hecho y de derecho de la decisión, que es lo que el artículo 36 exige y lo que, según la jurisprudencia citada en el considerando décimo tercero, no puede suplirse con la mera



relación de los antecedentes o de las solicitudes de los intervinientes. Que la defensa no pueda cotejar por ahora esos antecedentes con la solicitud que los contiene no es una falta de la resolución, sino una consecuencia de la reserva que el Ministerio Público decretó el 24 de julio de 2026 con arreglo al artículo 31 de la Ley N° 19.913, norma que permite mantener la investigación en secreto respecto del imputado por un plazo máximo de seis meses, renovable por una sola vez con autorización del juez de garantía, y que, en tanto disposición especial, prevalece sobre las reglas generales de acceso a la carpeta judicial, como lo entendió la jueza recurrida al negar las copias pedidas en la audiencia, decisión que el recurso no impugna. Levantado o limitado el secreto, el amparado podrá controvertir la suficiencia de esos antecedentes por las vías que la ley le franquea. En lo que el recurso sí acierta es en que la resolución, al autorizar el acceso a toda la información de los dispositivos y de los servicios vinculados a ellos, omitió determinar el objeto de la revisión, defecto que se ha examinado en los considerandos décimo tercero y siguientes, que la resolución de 26 de agosto no corrigió y que las medidas que se dispondrán subsanan. Como el propio recurrente no pide que se deje sin efecto la incautación ni que se impida el acceso al contenido de las especies, sino que éste quede circunscrito a lo que la investigación requiere, ese resultado se alcanza complementando la resolución que se pronunció sobre la cautela de sus garantías, que fue la oportunidad en que el tribunal debió fijar esos límites, sin necesidad de un pronunciamiento separado sobre la autorización de 19 de agosto, cuya ejecución quedará regida por dichas medidas. Lo mismo vale para la inconsistencia que el recurso denuncia entre el marco fijado para la incautación y la amplitud del acceso autorizado, pues los criterios de búsqueda que se ordenará proponer deberán determinarse, precisamente, por los hechos investigados.

En cuanto a los artículos 218 y 223 del Código Procesal Penal, la recurrida tiene razón en que la selección de lo pertinente que ambos ordenan presupone el examen del material y no una prohibición de examinarlo, y por eso las medidas que se disponen no impiden la revisión de la copia, sino que la someten a criterios previos y a un control posterior. Pero de que el examen sea inevitable no se sigue que pueda practicarse sin criterios ni que lo impertinente pueda permanecer indefinidamente en poder



del persecutor, que es lo que la resolución de 26 de agosto dejó abierto. El inciso final del artículo 218, que ordena al fiscal conservar únicamente la correspondencia relacionada con el hecho investigado y devolver la restante, y el inciso cuarto del artículo 223, que manda destruir las copias de las comunicaciones impertinentes, expresan la misma regla sobre el destino de lo que no interesa a la investigación que, según se dijo en el considerando décimo cuarto, fundamenta la eliminación del excedente de la copia.

La alusión del recurso, y del informe que lo responde, a los respaldos íntegros de tres casillas de correo institucionales no encuentra correlato en los antecedentes de este amparo, que versa sobre los dispositivos incautados al amparado, y la resolución de 19 de agosto tampoco invocó el artículo 218, sino los artículos 181, 187, 205, 209 y 217 del Código, lo que no altera lo dicho.

Vigésimo tercero: Que lo que se resolverá no busca limitar ni obstaculizar la investigación del Ministerio Público, sino alcanzar el equilibrio entre la eficacia de la persecución penal y el respeto de los derechos fundamentales que la Constitución exige en toda diligencia intrusiva. La extracción y el análisis del contenido de los dispositivos podrán continuar; la delimitación de los hechos, del período y de las personas de interés seguirá siendo propuesta por el persecutor; y ningún antecedente pertinente a los hechos investigados quedará fuera de su alcance. Lo único que se agrega es aquello que el legislador ya impone a diligencias de intensidad comparable, esto es, un plazo, un objeto determinado, la destrucción de lo que no sirve y una oportunidad para que el juez verifique que así se hizo. Ese es el sentido del artículo 10 del Código Procesal Penal cuando faculta al juez para adoptar las medidas necesarias para el ejercicio de las garantías, y del artículo 14 letra a) del Código Orgánico de Tribunales cuando le encomienda asegurarlas. Esta Corte no desconoce que se trata de un control que los tribunales no han practicado, o sólo excepcionalmente, respecto de una diligencia que la ley no regula. Por eso las medidas que se adoptan son las que parecen razonables y prudentes para restablecer el equilibrio buscado, en la expectativa de que resulten suficientes; pero, dada la dificultad de la materia, el mismo juzgado de garantía podrá revisarlas, de oficio o a petición de cualquier interviniente, cuando su ejecución muestre



que son insuficientes para proteger los derechos comprometidos o que entorpecen innecesariamente la investigación, y hacer los ajustes que ese equilibrio requiera.

Vigésimo cuarto: Que, conforme a lo razonado, la resolución de 26 de agosto de 2026, en cuanto rechazó fijar límites a la ejecución de la extracción y revisión del teléfono y de los demás dispositivos incautados al amparado más allá de los que consignó, y remitió el resguardo de la información impertinente y privada a instructivos internos del persecutor y a una eventual exclusión probatoria futura, no satisfizo las exigencias que los artículos 5°, 9°, 10 y 36 del Código Procesal Penal y 14 letra a) del Código Orgánico de Tribunales imponen al juez de garantía, y dejó subsistente una afectación cierta y actual de la vida privada del amparado y de la inviolabilidad de sus comunicaciones y de las de terceros, sobre la cual, conforme a lo resuelto por la Corte Suprema, corresponde a esta Corte pronunciarse derechamente, y que debe hacer cesar. En un caso semejante, el máximo tribunal ha estimado que exponer a la imputada a pesquisas investigativas sin la adopción de medidas de contrapeso que resguarden sus garantías fundamentales amenaza indebidamente su libertad personal y afecta de manera ostensible su derecho a la intimidad (SCS rol 49.866-2026, 24 de septiembre de 2026). Las medidas que se dispondrán siguen las líneas de ese precedente, con el apoyo que la regla del inciso cuarto del artículo 223 presta a la eliminación del excedente de la copia, y agregan la fijación de un plazo y de una audiencia de control. La identificación de la información útil deberá completarse dentro de noventa días contados desde la notificación de esta sentencia, plazo que sólo podrá ampliarse por una vez, por resolución fundada dictada en audiencia, para que por esa vía no se eluda el control ni se prolongue la conservación de la copia; y la audiencia en que se verificará lo obrado y se dispondrá la eliminación se celebrará dentro de los diez días siguientes, con citación de la defensa del amparado. La reserva de la investigación decretada con arreglo al artículo 31 de la Ley N° 19.913 no es obstáculo para ello. Esa norma permite mantener en secreto la investigación respecto del imputado, pero la audiencia versará sobre la conservación de las copias del contenido de sus propios dispositivos, que él obviamente conoce, y sobre los descriptores con que se acota la búsqueda y la información que se estima



impertinente, cuya revelación no compromete de modo relevante el secreto ni el éxito de la investigación, menos aún cuando los delitos que se indagan constan en los escritos públicos de este amparo y las defensas conocen los hechos desde la audiencia de cautela de garantías. Diferir el control hasta el término de la reserva, que puede extenderse por un año, sería una forma de eludirlo. Durante ese plazo el persecutor y la policía trabajarán sobre la copia íntegra para identificar lo pertinente; completada la identificación, y hasta que la audiencia resuelva sobre la eliminación, la copia quedará sellada y sin acceso, porque desde ese momento el examen ha concluido y el persecutor sólo necesita la información que separó como relacionada con los hechos, de modo que en el lapso que media entre el término del examen y la audiencia la retención deja de ser una intromisión en curso.

Así, el amparo será acogido sólo en cuanto se dispondrán las medidas de control que se indicarán, y rechazado en lo demás, sin costas.

Por estas consideraciones y de conformidad, además, con lo dispuesto en el artículo 21 de la Constitución Política de la República y en el Auto Acordado de la Excm. Corte Suprema sobre Tramitación y Fallo del Recurso de Amparo, **se acoge**, sin costas, el recurso de amparo deducido por el abogado Samuel Donoso Boassi en favor de Darío Calderón González, en contra del Cuarto Juzgado de Garantía de Santiago, sólo en cuanto se declara que la resolución dictada el 26 de agosto de 2026 en la causa RUC 2600858361-6, RIT O-6719-2026, debe complementarse con las siguientes medidas, que dicho tribunal deberá adoptar y controlar:

a) El Ministerio Público informará al Cuarto Juzgado de Garantía de Santiago, dentro de quince días, el estado de la extracción y de la revisión ya practicada, la individualización de los funcionarios y peritos que han tenido y tendrán acceso a las copias obtenidas del teléfono y de los demás dispositivos incautados al amparado, y propondrá los criterios de búsqueda con que se practicará el análisis de la totalidad de lo extraído, incluidas las comunicaciones de las aplicaciones de mensajería, del correo electrónico y de las redes sociales, sean palabras clave, interlocutores, cuentas, tipos de archivo u otros descriptores, determinados por los hechos investigados, por el período comprendido entre el año 2018 y el 20 de agosto de 2026 ya fijado en la resolución recurrida y por las personas, números o cuentas de interés para la investigación, sin perjuicio de su posterior complementación



con conocimiento del tribunal. Esos criterios excluirán las comunicaciones y documentos relativos a los clientes del amparado en el ejercicio de su profesión de abogado en asuntos ajenos a los hechos investigados, sin perjuicio de que las comunicaciones alcanzadas por los criterios de búsqueda, por relacionarse con esos hechos, puedan ser examinadas y conservadas cualquiera sea su interlocutor; si el Ministerio Público tuviere antecedentes para estimar que en las comunicaciones excluidas hay también elementos útiles para la investigación de los delitos de esta causa, deberá justificarlo determinadamente ante el juez de garantía, quien resolverá. Quedarán excluidas de la búsqueda, y serán eliminadas de la copia, las comunicaciones del amparado con sus abogados defensores, en esta o en otras causas, relativas al ejercicio de su defensa, a menos que el abogado respectivo fuere imputado por los hechos investigados. El juez de garantía apreciará la precisión y razonabilidad de los criterios propuestos y podrá exigir su acotamiento. Los dispositivos incautados y las copias obtenidas de ellos permanecerán bajo la custodia exclusiva del fiscal adjunto a cargo de la investigación.

b) La identificación de la información útil para la investigación deberá completarse dentro de noventa días contados desde la notificación de esta sentencia. El juez de garantía podrá ampliar ese plazo por una sola vez, por resolución fundada dictada en audiencia a la que se citará a la defensa del amparado, previo informe del Ministerio Público sobre el estado de la diligencia; la ampliación no suspenderá las demás medidas de esta sentencia. Vencido el plazo o su ampliación, el Ministerio Público separará en un soporte distinto la información identificada como relacionada con los hechos investigados e informará de ello al tribunal, y las copias íntegras de los dispositivos quedarán desde entonces selladas, bajo la custodia del fiscal a cargo conforme al artículo 188 del Código Procesal Penal, sin acceso alguno hasta que el tribunal resuelva sobre su eliminación.

c) Dentro de los diez días siguientes al vencimiento del plazo de la letra b) o de su ampliación, el Cuarto Juzgado de Garantía de Santiago celebrará una audiencia, con citación de la defensa del amparado, en la que el Ministerio Público dará cuenta de la información que conservará por tener relación con los hechos investigados, incluida, en su caso, la obtenida a través de las cuentas abiertas en los dispositivos a que se refiere la letra f),



y en la que el tribunal dispondrá la eliminación de las copias íntegras selladas y de toda otra información extraída que no haya sido identificada como pertinente, en particular la relativa a los clientes del amparado a que se refiere la letra a), de lo que deberá dejarse constancia mediante certificación que identifique el procedimiento seguido y a los funcionarios que lo practicaron, y resolverá sobre la devolución de los dispositivos al amparado o, si su conservación fuere necesaria, sobre su custodia. La reserva de la investigación decretada conforme al artículo 31 de la Ley N° 19.913 no suspenderá esta audiencia ni la intervención de la defensa del amparado en ella.

d) Hasta que se celebre esa audiencia, el Ministerio Público podrá utilizar en la investigación únicamente la información que identifique como relacionada con los hechos investigados. La información restante no podrá ser examinada más allá de lo necesario para su identificación, ni entregada a otros intervinientes o a terceros, ni incorporada a la carpeta investigativa ni a informes policiales, conforme a lo ya resuelto por el tribunal recurrido, y quedará comprendida en las copias selladas a que se refiere la letra b).

e) Si el Ministerio Público estimare que las copias contienen información relevante para hechos distintos de los investigados, deberá ponerlo en conocimiento del Cuarto Juzgado de Garantía de Santiago antes de utilizarla con cualquier fin, indicando el criterio o descriptor de búsqueda con que llegó a ella. El tribunal, con los criterios informados conforme a la letra a), verificará si se trató de un hallazgo casual, producido dentro de los límites de la orden y de una búsqueda razonable, y no de una revisión exploratoria del contenido en busca de delitos no determinados. Si lo estima así, autorizará su uso; en caso contrario, la información no podrá utilizarse en esta ni en otra investigación y será eliminada junto con el excedente de las copias conforme a la letra c). En caso de urgencia, la autorización podrá requerirse por la vía más rápida.

f) Las limitaciones anteriores rigen respecto de la totalidad de la información extraída, y en particular respecto de las aplicaciones de mensajería, del correo electrónico y de las redes sociales, que concentran las comunicaciones del amparado. Los criterios de búsqueda de la letra a) deberán determinar, para cada una de ellas, las cuentas, los interlocutores o contactos y el período cuyas comunicaciones podrán examinarse, y las



palabras clave o categorías de contenido a que se acotará la revisión, sin que puedan examinarse íntegramente conversaciones, casillas o perfiles de personas ajenas a los hechos investigados. Esas mismas limitaciones se aplican a la información que no está grabada en los dispositivos, sino almacenada en los servidores de esos servicios o en los de almacenamiento en la nube, y a la que los aparatos permiten ingresar directamente por mantener abierta la sesión de la cuenta respectiva, acceso que la resolución de 19 de agosto de 2026 autorizó en términos genéricos; a su respecto, el Ministerio Público informará además al tribunal, en el plazo de la letra a), a qué servicios y cuentas ha accedido o pretende acceder por esa vía, para que el juez de garantía determine el alcance de ese acceso con arreglo a los artículos 225 bis y 225 ter del Código Procesal Penal, y fuera de lo así informado y autorizado no podrá ingresarse a esos servicios a través de las cuentas abiertas en los aparatos.

g) Las fotografías, videos y audios contenidos en los dispositivos o accesibles a través de las cuentas abiertas en ellos, cuyo contenido no puede seleccionarse mediante palabras clave, se examinarán con sujeción al período fijado y a su procedencia, ordenando la revisión a partir de los archivos adjuntos a las conversaciones, correos o cuentas comprendidos en los criterios de búsqueda. Dentro de ese universo la revisión será directa y la practicarán únicamente los funcionarios individualizados conforme a la letra a), sin generar copias adicionales, dejando constancia de los archivos que se conserven por su relación con los hechos investigados; los restantes, incluidos los de carácter personal y familiar, quedarán comprendidos en la eliminación de la letra c).

h) El Cuarto Juzgado de Garantía de Santiago podrá, de oficio o a petición de cualquier interviniente y por resolución fundada dictada en audiencia, ajustar las medidas anteriores cuando su ejecución muestre que resultan insuficientes para resguardar los derechos comprometidos o que entorpecen innecesariamente la investigación.

Acordada con el voto en contra del ministro (s) señor Rodrigo Carrasco, quien fue del parecer de rechazar el recurso de amparo, por estimar que las resoluciones impugnadas no adolecen de la ilegalidad que se les atribuye, por cuanto fueron dictadas por el tribunal de garantía competente, en el marco de una investigación penal, en un proceso



legalmente tramitado, en ejercicio de las facultades que la ley le confiere a la referida magistratura y se encuentran debidamente fundadas en los antecedentes de la investigación.

En efecto, la primera autorizó la incautación y revisión de dispositivos electrónicos con fundamento en los antecedentes de la causa, conforme a los artículos 9, 181, 187 y 217 del Código Procesal Penal, y la segunda, pronunciada en audiencia de cautela de garantías, acotó temporalmente la búsqueda de información en el dispositivo incautado y prohibió incorporar a la carpeta investigativa o entregar a terceros información ajena a los hechos investigados.

A mayor abundamiento, cabe consignar que aún si se soslayara lo anterior, a juicio de este disidente, no se advierte de qué modo lo resuelto priva, perturba o amenaza la libertad personal o seguridad individual del amparado, únicas garantías fundamentales susceptibles de ser tuteladas a través de la acción deducida, en los términos previstos en el artículo 21 de la Constitución Política de la República.

Regístrese, notifíquese y archívese.

Redacción del ministro Manuel Rodríguez Vega y del voto en contra, su autor.

Regístrese, notifíquese y archívese.

N° Amparo-4294-2026.-



Manuel Esteban Rodríguez Vega
Ministro
Corte de Apelaciones
Veintinueve de septiembre de dos mil veintiséis
13:08 UTC-3





Rodrigo Alejandro Carrasco Meza
Ministro(S)
Corte de Apelaciones
Veintinueve de septiembre de dos mil veintiséis
13:01 UTC-3





Sebastián Esteban Perello Enrich
Abogado
Corte de Apelaciones
Veintinueve de septiembre de dos mil veintiséis
13:05 UTC-3



Pronunciado por la Sexta Sala de la C.A. de Santiago integrada por Ministro Manuel Esteban Rodríguez V., Ministro Suplente Rodrigo Alejandro Carrasco M. y Abogado Integrante Sebastián Esteban Perelló E. Santiago, veintinueve de septiembre de dos mil veintiseis.

En Santiago, a veintinueve de septiembre de dos mil veintiseis, notifiqué en Secretaría por el Estado Diario la resolución precedente.



Este documento tiene firma electrónica
y su original puede ser validado en
<http://verificadoc.pjud.cl>

Código: GFPXDXZYNUP