LA OBTENCIÓN DE LA PRUEBA Y SU TENSIÓN CONSTITUCIONAL EN LA ERA DIGITAL: CRÍTICA A LOS LÍMITES CLÁSICOS DE LA GARANTÍA CONTRA LA AUTOINCRIMINACIÓN

Tomás Camilletti

1. INTRODUCCIÓN

El avance de la tecnología no sólo ha modificado de gran manera la vida cotidiana de las personas a nivel global, sino también en lo que respecta a las implicancias que pueda llegar a tener ello en su esfera privada y su relación con el derecho.

Así pues, observamos cómo hoy en día mediante dispositivos tecnológicos las personas pueden comunicarse, almacenar datos de información valiosa, hasta incluso contar con su documentación personal como cédulas de identidad, licencias de conducir, billeteras virtuales, tarjetas de crédito, en fin, un sinnúmero de aplicaciones con las que se puede convivir o crear una nueva forma de estructurar la vida.

Pues bien, teniendo en consideración que el derecho positivo evoluciona a una velocidad considerable y las realidades cotidianas mutan y deben ir adaptándose a los cambios, vemos como tales cuestiones no fueron (ni son) ajenas al derecho penal y procesal penal. En ese sentido, dentro del universo de cuestiones en los que incide la tecnología a la hora de investigar hechos ilícitos, lo cierto es que el uso de *smartphones* ha incorporado un nuevo paradigma en la obtención de elementos probatorios, circunstancia la cual trajo una serie de cuestionamientos los cuales pretendo describir sucintamente por medio de este trabajo.

Y estos son, en el particular, los límites constitucionales con los que cuenta hoy en día el acceso compulsivo sobre estos dispositivos y parte de la tensión que ello recepta con la garantía contra la autoincriminación.

En esta línea, pretendo no sólo poner de manifiesto algunas de las discusiones clásicas brindadas en torno a la validez constitucional del desbloqueo compulsivo de los *smartphones* (sea cual fuera la forma de acceso), sino también intentar dejar planteada la problemática que se presenta a nivel estructural en torno al abordaje de estas cuestiones dentro de las investigaciones penales, la necesidad de reinterpretar el alcance de esta garantía frente al avance de las nuevas herramientas de investigación y el juego armónico que debe existir con ello en pos de tornar eficaces los procesos y respetuosos de la dignidad humana.

En ese sentido, partiré de la hipótesis de insuficiencia de los criterios doctrinarios que delimitan el alcance del *nemo tenetur* para satisfacer los derechos y garantías de las personas sometidas al proceso penal, entendiendo que el acceso forzado a los dispositivos -ya sea con clave alfanumérica o mediante reconocimiento facial-, implica una nueva forma de intervención estatal que bien puede desdibujar los límites del debido proceso y transformar así al imputado como fuente directa de prueba incriminante.

Y esto es así, debido a que -como veremos- la vida digital de la persona contenida en un dispositivo tecnológico implica mucho más que un mero “mecanismo” por el cual se almacenan datos personales -formando parte de la vida privada de los individuos-, por lo que la intromisión por parte de los organismos Estatales mal puede efectuarse a cualquier costo, independientemente de la riqueza probatoria que los mismos pudieran tener.

En este aspecto, se propondrá incorporar las transformaciones que trae aparejada la digitalización de la vida cotidiana, desde una perspectiva dogmática crítica e intentando explorar nuevos conceptos y espacios que merecen protección constitucional y que, hoy en día solo terminan siendo “parches” y/o reinterpretaciones sobre doctrinas clásicas que van quedando obsoletas a la hora de abordar, en el caso, las situaciones en las cuales el Estado accede coactivamente a los dispositivos de las personas y consecuentemente, a la información privada de éste sin que haya mediado manifestación de voluntad alguna, incorporando la evidencia obtenida al proceso y tornándose ello en prueba ilícita.

Desde el punto de vista metodológico, haré un análisis descriptivo sobre algunas cuestiones teóricas y el avance que ha receptado la jurisprudencia argentina y norteamericana a lo largo de los años, intentando con ello proponer algunos criterios rectores que podrían echar luz a esta problemática evidenciada para así poder reflotar el garantismo del proceso penal ante la coexistencia de los entornos digitales.

A modo de conclusión lo que se intentará confirmar es que el avance tecnológico no sólo trajo aparejados nuevos desafíos en torno a nuevas figuras delictivas y formas de criminalidad, sino que también ello se ha traducido en nuevos horizontes en materia probatoria, debiendo pensarse indefectiblemente en clave constitucional, teniendo en consideración que los dispositivos telefónicos inteligentes de las personas no son más que una puerta de entrada privilegiada a la esfera íntima del sujeto sometido a proceso y, por consiguiente, su acceso compulsivo ya sea por la introducción de un código o bien sus datos biométricos, una forma de aportarle al Estado prueba de cargo en flagrante transgresión a derechos constitucionalmente protegidos.

2. FUNDAMENTOS Y LÍMITES CLÁSICOS A LA GARANTÍA CONTRA LA AUTOINCRIMINACIÓN

Como he anticipado, el límite al acceso a la información contenida en un teléfono celular o dispositivo inteligente está dado por las nuevas formas de encriptación y seguridad que tienen los mismos. Y si bien no resultaría cuestionada la aseveración que para acceder a los mismos en el marco de una investigación resulta exigible una orden judicial¹, lo cierto resulta ser que la cuestión se complejiza cuando pese a ello, el acceso a la información se encuentra sujeto al desbloqueo exclusivo por parte de la persona investigada, ya sea mediante huellas digitales, claves alfanuméricas y/o mediante los datos biométricos.

Pues bien, entendiendo que el marco legal actual no se ha podido adaptar a la realidad que presenta la evidencia digital hoy en día, la doctrina y la jurisprudencia -principalmente la norteamericana- ha brindado a lo largo del tiempo una serie de parámetros específicos a la hora de validar -o no- este tipo de injerencias en la esfera privada de las personas.

En este aspecto entiendo que las cuestiones planteadas presentan tres problemáticas relevantes que tornan, cuanto menos, cuestionables ciertas conductas en el transcurso de una investigación penal:

a) Por un lado, la misión epistémica del proceso y la búsqueda de la verdad frente a los derechos constitucionalmente protegidos de las personas sometidas a proceso, dado que entiendo que no se puede obtener la verdad real a cualquier costo, teniendo en consideración que las garantías constitucionales actúan como un "escudo protector del ciudadano frente al poder penal"².

b) En segundo lugar, el principio de libertad probatoria frente a los límites concretos que hoy existen. En ese sentido, de la experiencia en los sistemas procesales estudiados y lo que puede observarse en torno a los argumentos brindados por los organismos encargados de llevar adelante la investigación (y los jueces que habilitan dichas injerencias), entiendo que esa "libertad probatoria" mal puede ser una "excusa" para avasallar derechos constitucionalmente protegidos³. Máxime cuando la interpretación dominante que busca excluir la prueba ilícita se ha demostrado insatisfactoria frente a las nuevas tecnologías, dejando al arbitrio judicial la determinación de su licitud.

¹ Ver *Riley vs. California*, SCOTUS 573 U.S. 373 (2014). En similar sentido se expidió la Corte Interamericana de Derechos Humanos (CIDH), *Caso Escher y Otros vs. Brasil*; Sentencia de 6 de julio de 2009 (Excepciones Preliminares, Fondo, Reparaciones y Costas); párr. 113-115; 129.

² FAVAROTTO, R. S.; "El derecho a oponerse a colaborar con la acusación"; Publicado en: DPyC, 2025 (febrero), 93, Argentina. Cita: TR LALEY AR/DOC/65/2025. También desarrollado en BINDER, A., *Introducción al derecho procesal penal*, 2da. Ed. actualizada y ampliada, Ad Hoc, Ciudad de Buenos Aires, 2016, pp. 56/64.

³ SALT, M. "Allanamiento remoto ¿Un cambio de paradigma en el registro y secuestro de datos informáticos?", en *Cibercrimen II*, 1a edición, Ed. BdeF, Montevideo-Buenos Aires, 2018, pp. 151/181.

c) Por último, como anticipé, la problemática vinculada con la ausencia de una regulación legal específica para la materia y la aplicación analógica de las normas relativas a otros medios de prueba -que no contemplan la prueba digital-, que bien podría transgredir el principio de legalidad, puesto que toda injerencia estatal que afectara derechos fundamentales debe llevarse adelante bajo los estrictos términos legales establecidos y, asimismo, por una ley previa, clara y precisa⁴. Aquí juega un papel fundamental el principio *nulla coactio sine lege*, por cuanto ello y el principio de libertad probatoria de las partes, entran en franca tensión⁵.

Ahora bien, veamos algunas cuestiones teóricas:

Debe destacarse que dentro del ordenamiento jurídico en el cual se lleva adelante este análisis, el principio de la autoincriminación forzada (*nemo tenetur se ipsum accusare*) se encuentra dispuesto en el artículo 18 de la Constitución Nacional y en tratados internacionales de derechos humanos, tales como el art. 8.2.g de la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica) y el art. 14.3.g del Pacto Internacional de Derechos Civiles y Políticos, entre otros.

En lo que respecta a su tratamiento jurisprudencial en la región, la Corte Suprema de Justicia de la Nación Argentina (en adelante “CSJN”), en casos como *Mendoza* (1864) hasta *Diario El Atlántico* (1971), ha interpretado que cualquier forma de coacción -física o moral- que obtenga una confesión vulnera la garantía. Sin embargo, en precedentes como *Cincotta* (1963), *H. G. S.* (1995) o más recientemente en *Rau* (2016) el Tribunal introdujo distinciones que habilitaron la obtención compulsiva de evidencia “material” (reconocimiento en rueda, extracción de muestras, firmas) al considerar que el imputado pasaba a ser “objeto” y no “sujeto” de prueba⁶.

Esta discusión brindada en el plano doctrinario y jurisprudencial giró en torno a tres binomios que llevaron -aunque quizás de manera infructuosa ante el avance tecnológico- a discutir y delimitar el alcance de la presente garantía y poder interpretar cuándo un acto se encuentra cubierto por la misma o no. Y esto se llevó a cabo mediante las clásicas distinciones del imputado como **1) sujeto de prueba** y *como objeto de prueba*; **2) la actividad** del imputado o la *pasividad*; y por otro lado **3) la manifestación testimonial** o la *prueba física*.

Según los partidarios de la **primera distinción**, la garantía contra la autoincriminación protege al imputado cuando actúa como sujeto que aporta conocimientos incriminantes por medio de una declaración -oral o escrita- cuya exteriorización depende de su voluntad. En estos casos, la prueba se halla en su fuero interno, en su mente, y su producción requiere un acto volitivo. Contrariamente a ello, dicha protección no se extiende cuando el imputado es considerado un mero objeto sobre el cual se practican ciertas diligencias probatorias -como la extracción de sangre o huellas, ruedas de reconocimiento, etc.-, en tanto éstas no implican una exteriorización de su pensamiento.

Por otra parte, en relación con la dicotomía de **actividad o pasividad** de la persona imputada, la garantía rige cuando ésta actúa como "sujeto u órgano de prueba", es decir, cuando proporciona activamente un conocimiento a través de una declaración o manifestación consciente y voluntaria -sea verbal, escrita o gestual-. En estos supuestos, toda coacción destinada a obtener contenido de carácter comunicativo o declarativo se encuentra prohibida, por depender su exteriorización exclusivamente de la voluntad del individuo. Por ejemplo, exigir una clave alfanumérica o un patrón de desbloqueo de un teléfono se considera generalmente una “actividad” y, por tanto, protegido por esta garantía, lo que implicaría que el imputado podría negarse a proporcionarlos.

Por el contrario, cuando el imputado es portador material de los elementos probatorios -y por ende tratado como objeto de prueba-, la doctrina tradicional considera que la garantía no resulta

⁴ PÉREZ BARBERÁ, G., “Nuevas tecnologías y libertad probatoria en el proceso penal”, en *Nueva Doctrina Penal*, Ed. del Puerto, Argentina, 2009/A, pp. 271 y sgts.

⁵ BRUZZONE, Gustavo, “La *nulla coactio sine lege* como pauta de trabajo en materia de medidas de coerción en el proceso penal”, AA.VV. *Estudios sobre Justicia Penal, Homenaje al Profesor Julio B. J. Maier*. Editores del Puerto, Buenos Aires, 2005, pp. 241/253.

⁶ En este sentido resulta ilustrativo el análisis jurisprudencial efectuado por CARRIÓ A. en su obra *Garantías Constitucionales en el proceso penal*, 6ta. Ed., 6ta. Reimp., Ed. Hammurabi, Argentina, 2023, pp. 483/555, a la cual en honor a la brevedad me remito, destacando la claridad expositiva y riqueza que se extrae de la obra del autor.

aplicable. En estos casos, se le exige al imputado una "tolerancia" pasiva, es decir, que su cuerpo sea utilizado como fuente de evidencia física, sin que el acto implique la exteriorización de un pensamiento o conciencia⁷.

Y, en tercer lugar, puede señalarse que un razonamiento análogo ha sido proyectado sobre la tradicional distinción entre prueba **testimonial** y prueba **física**. La garantía contra la autoincriminación ha sido históricamente asociada a la prohibición de compeler al imputado a producir prueba de carácter testimonial o comunicativo. En estos casos, el imputado es considerado nuevamente como "sujeto de prueba", y cualquier forma de coacción destinada a obtener información que surja de sus procesos mentales -como obligarlo a declarar, a redactar un cuerpo de escritura, o a proporcionar una clave alfanumérica o patrón de desbloqueo- se encuentra constitucionalmente vedada.

Por el contrario, cuando se trata de la llamada "prueba física" o "prueba real", se sostiene que la garantía no resulta aplicable. En tales supuestos, el imputado es concebido como un "portador material" de los elementos probatorios, y se le exige una actitud pasiva o un deber de tolerancia frente a diligencias que no implican la exteriorización de su voluntad o pensamiento, tales como la toma de muestras biológicas, la extracción de huellas digitales o la participación en ruedas de reconocimiento.

Pero, ¿qué sucede frente a los desbloques compulsivos de teléfonos celulares? ¿Es lo mismo aportar un patrón, colocar una huella digital o desbloquearlo por medio de datos biométricos?

Habiendo repasado sucintamente los fundamentos clásicos que giran en torno al alcance de la presente garantía, se intentará poner en evidencia cómo la doctrina y la jurisprudencia aún no han podido aportar fundamentos suficientes que puedan sellar la controversia existente ante el avance de la prueba digital en el mundo, intentando ilustrar cómo es que con el desbloqueo compulsivo de los dispositivos electrónicos, dicha garantía puede verse amenazada.

3. BREVES REFERENCIAS JURISPRUDENCIALES: ENTRE LA LAGUNA NORMATIVA Y LA CREATIVIDAD JUDICIAL

A modo ilustrativo, la Suprema Corte de los Estados Unidos (en adelante "SCOTUS") fijó inicialmente los alcances de los intereses amparados por la 5ta. Enmienda en el popular *leading case* *Miranda*.

En la misma, la SCOTUS señaló que el fundamento constitucional que subyace bajo la garantía contra la autoincriminación, radica en el respeto que todo gobierno debe otorgar a la dignidad e integridad de las personas, como condición indispensable para preservar un equilibrio justo entre el poder estatal y los derechos individuales. En este marco, estableció que se impone al Estado la obligación de asumir plenamente la carga de la prueba, obteniendo la evidencia de manera autónoma y sin vulnerar la inviolabilidad de la persona humana. Esta exigencia responde al principio estructural del sistema acusatorio, que prohíbe al Estado recurrir al mecanismo cruel de forzar al imputado a proveer, con sus propias palabras, los elementos que lo incriminan⁸. Así pues, refirió que la garantía se satisface cuando a la persona se le garantiza el derecho a permanecer callado a menos que elija declarar sin restricciones en el ejercicio de su propia voluntad. En Estados Unidos, para el caso, vendría a ser una suerte de renuncia al derecho de quedarse callado y, consecuentemente, a no autoincriminarse, pero pareciera ser que la realidad del año 1966 dista mucho de la que hoy en día nos podemos encontrar.

Sin embargo, en el mismo año la Corte se expidió en el caso *Schmerber*⁹, en donde introdujo una distinción que marcaría el rumbo de la postura imperante hoy en día en la materia, comenzando a delinear el alcance de la presente garantía ante la presencia de evidencia documental.

⁷ CARRIÓ, A., *Garantías constitucionales...*; pp. 546/549; BUGLIONE, M. J.; "El desbloqueo forzoso de celulares. Validez constitucional y estado actual de la jurisprudencia", Revista Temas de Derecho Penal, Errepar, Argentina, 05-08-2024.

⁸ SCOTUS 384 U.S. 436 (1966), párr. 42.

⁹ SCOTUS 348 U.S. 757 (1966).

En dicho precedente, el Tribunal norteamericano manifestó que la garantía protege al imputado de ser obligado a declarar contra sí mismo, o a aportarle al Estado evidencia de naturaleza testimonial o comunicativa, mas que la compulsión a extraerse huellas digitales, fotografías, cuerpo de escritura, entre otras diligencias, no encuentra acogida suficiente en la 5ta Enmienda, dado que son fuentes de evidencia física o real -no comunicativa-¹⁰. Pues bien, como veremos, esta separación entre lo que se dice/lo que se es permitiría años más tarde utilizarse de manera análoga ante el acceso compulsivo a los dispositivos electrónicos.

Siguiendo con el análisis, con el correr de los años, la SCOTUS fue precisando esta línea divisoria y en *Fisher*¹¹ abordó el problema generado en torno a la documentación incriminatoria creada voluntariamente. En ese sentido la Corte sostuvo que la 5ta. Enmienda no protege ese tipo de evidencia escrita (dado que la garantía sólo actúa cuando lo que se pretende obtener es una comunicación testimonial, incriminatoria y compulsiva, que transmite o revela información al Estado), salvo que su presentación compulsiva implicara un aspecto comunicativo: una afirmación implícita sobre la existencia, posesión o autenticidad de esos documentos.

Sin embargo, la importancia de este precedente no radicó en la línea jurisprudencial que ya se venía gestando al respecto, sino que estableció una “excepción a la excepción”: si el Estado ya conoce de antemano la existencia de la evidencia, entonces el acto de entrega no transmite información nueva y, por lo tanto, no sería testimonial a los efectos del amparo en la 5ta. Enmienda. Es la llamada doctrina de la *foregone conclusion*, la cual afirma que no hay violación de la garantía cuando el contenido implícito del acto requerido ya es una “conclusión previsible” para la autoridad estatal. En simples palabras: como el Estado ya sabía, no había “comunicación de información” alguna¹², por lo que la garantía no operaba.

Esta excepción, como era de esperarse, dio lugar a nuevas disputas. Los precedentes *Doe I* (465 U.S. 605, 1984) y *Doe II* (487 U.S. 201, 1988) también constituyeron hitos en la distinción entre el contenido testimonial y los actos meramente mecánicos. En *Doe I*, la SCOTUS reconoció que, si bien los documentos preexistentes pueden no gozar de la protección pese a haber sido creados voluntariamente, el acto mismo de producirlos puede ser testimonial, en tanto implica una afirmación implícita sobre su existencia, posesión y autenticidad. Así, la protección no recae sobre el contenido documental en sí, sino sobre la dimensión expresiva del acto de entrega.

Por el contrario, en *Doe II*, la Corte consideró que requerir la firma de formularios de autorización de acceso a registros bancarios mantenidos por terceros no violaba la 5ta. Enmienda, ya que no implicaba una admisión personal de conocimiento ni control sobre los datos y, por tanto, carecía de contenido testimonial relevante. En este último, la Corte concluyó que la autorización brindada carecía de contenido testimonial, dado que, aunque el documento le otorgaba al Estado el acceso a una fuente potencial de evidencia, la autorización en sí misma no le indicaba a la acusación

¹⁰ La Corte refirió que "Es claro que la protección del privilegio alcanza a las comunicaciones del acusado, cualquiera sea la forma que adopten, y a la compulsión de respuestas que también constituyen comunicaciones, por ejemplo, el cumplimiento de una citación para presentar documentos propios. *Boyd v. United States*, 116 U. S. 616. Por otro lado, tanto los tribunales federales como los estatales han sostenido usualmente que dicho privilegio no ofrece protección contra la compulsión a someterse a la toma de huellas digitales, fotografías o mediciones, a escribir o hablar para ser identificado, a comparecer ante el tribunal, a ponerse de pie, adoptar una postura, caminar o realizar un gesto determinado. La distinción que ha surgido, a menudo expresada de diferentes maneras, es que el privilegio constituye un obstáculo frente a la compulsión de 'comunicaciones' o 'testimonios', pero que la compulsión que convierte al sospechoso o acusado en fuente de 'pruebas reales o físicas' no lo infringe" (La traducción es propia).

¹¹ SCOTUS, 425 U.S. 391 (1976).

¹² Ver también *U.S vs. Hubbel*, 530, U.S., 27 (2000). Autores como POLANSKY J. sostienen que “la doctrina de la *foregone conclusion* establece que la producción de una medida probatoria que resultaría violatoria de la garantía contra la autoincriminación resulta tolerable, desde una perspectiva constitucional, en aquellos casos en los que el Estado tiene conocimiento a priori de la información implícita que derivaría de la producción de la medida. En el caso del desbloqueo de teléfonos celulares mediante el ingreso compulsivo de datos biométricos, la medida resultaría tolerable constitucionalmente si el Estado, antes de proceder al desbloqueo, puede demostrar que conoce quién es su usuario y, por lo tanto, quién es el que posee el control sobre el contenido del dispositivo” (POLANSKY, J., *Garantías Constitucionales del Procedimiento Penal en el entorno digital*; Hammurabi, Buenos Aires, 2020, pp. 96).

la localización de cuentas bancarias ocultas ni tampoco aportaba información que pudiera asistirle en el descubrimiento de evidencia. El Estado debía localizar dichas pruebas mediante “la labor independiente de sus agentes”¹³.

Ahora bien, estas clásicas distinciones encontraron serios desafíos en el entorno digital y la jurisprudencia de tribunales inferiores en EEUU evidenció esas profundas divergencias.

Por tan solo mencionar algunos precedentes de relevancia, en el año 2014 el Tribunal del Segundo Circuito Judicial del Estado de Virginia se expidió en el caso *Baust*, donde consideró que el imputado podía ser compelido a apoyar su dedo y aportar su huella dactilar para desbloquear su teléfono, toda vez que ello carecía de contenido declarativo (testimonial)¹⁴, pero sin embargo otras decisiones más recientes asumieron una postura opuesta. En el caso “*Order denying application for a search warrant; order sealing application*” del Tribunal de Distrito Norte de California - Estados Unidos¹⁵, fue rechazada de manera contundente la orden de registro solicitada por el gobierno por considerar que éste no puede obligar o utilizar de otro modo los dedos, pulgares, el reconocimiento facial, óptico/iris, o cualquier otra característica biométrica para desbloquear dispositivos electrónicos¹⁶. Misma tesis adoptó el Tribunal del Distrito de Idaho en el año 2019¹⁷ o la Corte Suprema de Indiana en el caso *Katelin Eunjoo Seo*¹⁸, la cual advirtió sobre los peligros de extender la doctrina de la *foregone conclusion* a los teléfonos celulares. En este aspecto, expresó que “extender la excepción de la conclusión previsible a la producción obligatoria de un teléfono inteligente desbloqueado genera preocupación por tres razones: tal expansión (1) no tiene en cuenta la ubicuidad y capacidad únicas de los teléfonos inteligentes; (2) puede resultar inviable; y (3) va en contra de los precedentes de la Corte Suprema de EE. UU”, así como también que “la Corte Suprema en *Fisher, Doe o Hubbell*, seguramente no podía haber previsto que tales dispositivos llegarían a ser tan comunes o imaginado la amplitud y profundidad de la información que podrían contener”.

Ahora bien, en Argentina, además de los precedentes mencionados en el capítulo anterior que regulan el alcance de la garantía en la región -y si bien el desarrollo jurisprudencial en la materia aún resulta incipiente-, también se observan señales de esta tensión evidenciada. Resulta interesante mencionar un fallo dictado por la Cámara Federal de Bahía Blanca¹⁹, por cuanto pareciera ser que

¹³ SCOTUS, 487 U.S. 201, (1988). “Aunque el formulario firmado permite al Gobierno acceder a una posible fuente de prueba, la orden en sí misma no orienta al Gobierno hacia cuentas ocultas ni proporciona información que ayude a la fiscalía a descubrir pruebas. El Gobierno debe localizar esas pruebas ‘mediante el esfuerzo independiente de sus funcionarios’ (*Estelle v. Smith*, 451 U.S. 454, 462 [1981], citando *Culombe v. Connecticut*, 367 U.S. 568, 582 [1961], opinión que anuncia el fallo). [...]” (La traducción es propia).

¹⁴ Commonwealth of Virginia, Second Judicial Circuit, *Commonwealth of Virginia v. Baust*, Case Nro. CR-14-1439 (28/10/2014).

¹⁵ Ver en <https://repositorio.mpd.gov.ar/jspui/handle/123456789/5248> : Case N° 4-19-70053, 10/06/2019.

¹⁶ Aquí el tribunal expuso que “[...] los teléfonos móviles están sujetos a un tratamiento diferente al de los dispositivos de almacenamiento más tradicionales, como las cajas fuertes, y deben gozar de mayor protección”. [...] “De ello se deduce que cualquier argumento que sostenga que obligar a un sospechoso a proporcionar una característica biométrica para acceder a documentos y datos es sinónimo de presentar documentos en virtud de una citación judicial fracasaría. Como reconoció la Corte Suprema en el caso *Riley*, los teléfonos inteligentes contienen grandes cantidades de datos, incluidos datos de localización GPS y registros confidenciales, cuyo contenido íntegro no puede ser anticipado por las fuerzas del orden. Véase *Riley*. En consecuencia, el gobierno carece intrínsecamente del conocimiento previo necesario de la información y los documentos que podría obtener mediante un registro de estos dispositivos digitales desconocidos, de modo que no sería una cuestión de mera entrega. Véase *Hubbell*. Además, el gobierno sería incapaz de articular hechos para obligar al desbloqueo de dispositivos que utilizan características biométricas por parte de personas desconocidas que el gobierno no podría prever que estuvieran presente durante la ejecución de la orden de registro. De hecho, el pedido del registro de la fiscalía no hace ningún intento de hacerlo”.

¹⁷ Ver análisis del *Caso 1:19-mj-10441 REB* del Tribunal de Distrito de Idaho -EEUU- en MILLER, C. H., “¿Pueden las fuerzas de seguridad forzar el desbloqueo de un dispositivo con datos biométricos del sospechoso? Acerca de los recientes fallos de la justicia de los Estados Unidos”. Publicado en: LA LEY 03/07/2019, 6 • LA LEY 2019-C, 536. Argentina, 2019.

¹⁸ Ver en <https://repositorio.mpd.gov.ar/jspui/bitstream/123456789/5250/3/Katelin%20Eunjoo%20Seo.pdf> : Indiana Supreme Court; Supreme Court Case No. 18S-CR-595; *Katelin Eunjoo Seo -Appellant (Defendant) v. State of Indiana -Appellee (Plaintiff)-*; 23/06/2020.

¹⁹ Cámara Federal de Bahía Blanca, Expediente nro. FBB 3139/2022/1/CA1: “Incidente de Reposición: ‘MORA, Brisa Aylén por infracción ley 23.737 (art. 5 inc. c)’” de fecha 27/05/2022.

se inclinó por sostener la validez de la medida requerida, fundada ella en las doctrinas clásicas antes repasadas.

En este caso, en el marco de una causa donde se investigaba a la imputada por el almacenamiento de aproximadamente 500 kilos de marihuana y 5 kilos de cocaína, se le había requerido a la misma que aportara voluntariamente la clave de desbloqueo y, en caso de negativa, autorizar a un procedimiento compulsivo con mínima fuerza pública para obtener el patrón de desbloqueo dactilar o de iris y realizar un peritaje integral del dispositivo, por considerar que ésta, al ser "objeto de prueba", estaba obligada a someterse a la medida, la cual no resulta lesiva, degradante, y guardaba proporcionalidad con el fin perseguido, sin afectar la prohibición de autoincriminación del artículo 18 de la Constitución Nacional.

Llegado al tratamiento de la Cámara Federal de Bahía Blanca ante el recurso fiscal, el Tribunal, para resolver la cuestión de la autoincriminación, hizo una crucial distinción entre la prueba proveniente de declaraciones (cubierta por la garantía) y aquella en donde el imputado actúa como "objeto de prueba", soportando una injerencia corporal que no implique un trato degradante o humillante. Apoyándose en precedentes de la CSJN (como *Rau*²⁰), el fallo determinó que la garantía de no autoincriminación no abarca la evidencia de índole material, y que es posible extender este razonamiento a la obtención de características biométricas (huella dactilar, reconocimiento facial/iris) para desbloquear un dispositivo electrónico. El tribunal subrayó la necesidad de readecuar la interpretación de las herramientas procesales vigentes a la realidad de la era digital, para no caer en anacronismos y resguardar así el interés social en la persecución de delitos complejos como el narcotráfico, dada la gran cantidad de droga incautada.

Este razonamiento, sin embargo, reproduce sin mayor problematización la distinción clásica entre "lo físico" y "lo comunicativo", sin considerar que en el entorno digital ambos planos se entrelazan. Pues bien, se considera a los fines de esta presentación y así se mencionará en lo sucesivo, que **desbloquear un teléfono no es solo un acto físico: es, en muchos casos, una llave de acceso a la intimidad de una persona, por lo que, a mi criterio, ignorar esta dimensión equivaldrá a negar la naturaleza misma del problema.**

Para finalizar, la evolución jurisprudencial mencionada no hace más que revelar un escenario en evolución y constante cambio, donde los conceptos tradicionales se ven obligados a readecuarse con nuevas realidades tecnológicas. Mientras que en Estados Unidos se observa una proliferación de criterios disímiles y una peligrosa tendencia a ampliar excepciones como la *foregone conclusion*, en Argentina se advierte una incipiente adaptación que aún no alcanza a problematizar a fondo las consecuencias jurídicas de los actos tecnológicos. En ambos casos, el desafío consistirá en evitar que la creatividad judicial termine por vaciar de contenido una garantía que, en su origen, fue pensada precisamente para evitar que el Estado encuentre en el cuerpo o la conciencia del imputado el camino más corto hacia la condena.

4. INSUFICIENCIA DE LOS LÍMITES CLÁSICOS A LA GARANTÍA CONTRA LA AUTOINCRIMINACIÓN

En el apartado anterior pudimos observar cómo la jurisprudencia mayoritaria sustenta sus argumentos en torno al contenido testimonial de los actos del imputado, los cuales obtendrían -en estos casos- amparo concreto en torno al artículo 18 de la Constitución Argentina o bien la 5ta. Enmienda estadounidense. Ahora bien, la descryptación de los dispositivos por intermedio de una huella dactilar o el reconocimiento de los datos biométricos, ¿no podría tener contenido testimonial implícito?

²⁰ Recordemos que en *Rau* (Fallos 339:480), la Corte Suprema de Justicia de la Nación invocó los fundamentos brindados en *Cincotta* (Fallos 255:18) y *Zambrana Daza* (Fallos 320:1717), estableciendo que lo que transgrede la garantía en cuestión es la utilización de cualquier modo de coacción o artificio tendiente a obtener declaraciones inculpatorias que la persona no tiene la obligación de manifestar, no abarcando los supuestos donde la evidencia es de índole material y producto de la libre voluntad de la persona.

En este caso, entiendo al igual que autores como Polansky²¹, que quien desbloquea su dispositivo telefónico, de cualquiera de las formas previstas, estará indicando de manera tácita que ese teléfono y, por consiguiente, toda la información que allí sea hallada, le pertenece. El acto de desbloquear un celular con datos biométricos sí tiene un contenido declarativo o testimonial implícito, visto que, al hacerlo, el imputado está reconociendo la existencia, posesión, control y autenticidad de los documentos almacenados en el dispositivo.

En este aspecto, considero que independientemente del carácter testimonial o no de la garantía que prohíbe la autoincriminación coactiva, en la actualidad los dispositivos electrónicos cuentan con los registros de vida de todas las personas, por lo que no puede tratarse de una manera liviana o superficial dicha problemática. Como podrá advertirse, la doctrina estadounidense de la *foregone conclusion* no resultaría suficiente, visto que es inconmensurable e imprevisible la cantidad de datos que se podrían encontrar en un dispositivo moderno, por lo que incluso podríamos encontrarnos con problemas concernientes al cercenamiento de otras garantías constitucionalmente protegidas como, por ejemplo, la intimidad.

En este aspecto, el proceso penal y su fin último, el de buscar la verdad material, se ha visto superado con el advenimiento de las nuevas tecnologías, siendo a todas luces evidente que una interpretación lineal y semántica del artículo 18 de la Constitución Nacional Argentina no permite incluir las nuevas formas de producción de pruebas.

En esa línea, entiendo que se debe imponer una exégesis dinámica y progresiva de los derechos y garantías constitucionales que se encuentran en juego -en sintonía con el artículo 33 de la Constitución Argentina-, la cual permita equilibrar las injerencias a los derechos constitucionalmente protegidos ante el desafío que presenta la incorporación de nuevas tecnologías en la vida cotidiana de las personas. En pos de ello, entiendo que se debería privilegiar el método interpretativo que más derechos otorgue y proteja al ser humano frente al poder punitivo estatal²².

Tal como se mencionó anteriormente, tampoco puede hacerse caso omiso a la inconveniencia que deja relucir la aplicación analógica de normas y derechos ante estos espacios no regulados.

Como se ha analizado y tal como jurisprudencialmente ha intentado ser abordado, las similitudes entre la evidencia digital y la evidencia física, no dejan de ser tan solo una ficción, por lo que se puede observar que seguir sustentando fundamentos en criterios adoptados por organismos jurisdiccionales a mediados del siglo XX resulta cuanto menos peligroso. Entiendo que lo mismo sucede con el intento de aplicación de normas que rigen para los elementos de prueba tradicionales, lo cual como se podrá inferir, a mi criterio puede ser cuestionable desde una perspectiva constitucional y convencional, dejando librado al arbitrio judicial (en base a su interpretación), los límites a la injerencia estatal como también en la protección de ciertas garantías.

Es indiscutible que el imputado no tiene el deber de cooperar y ayudar a la acusación en la búsqueda de la verdad, por lo que la interpretación en casos como el presente resulta muy frágil ante el avance del poder estatal, debiendo establecer mínimamente ciertas bases que puedan brindarle seguridad jurídica a la persona sometida a proceso y limitar los avances del Estado sobre ésta. En tal sentido, debe verse de manera auspiciosa la posibilidad de establecer un “principio de incoercibilidad” como concepto totalizador que limite estas interpretaciones tan amplias en torno a la garantía contra la autoincriminación.

Autores como Gustavo Aboso han establecido que el principio de incoercibilidad se basa en la trilogía de autonomía-libertad-dignidad de la persona, que establece límites infranqueables a la injerencia en los derechos del imputado, y el cual tendrá como propósito ofrecer una base de fundamentación más amplia para rechazar las consecuencias negativas de una interpretación estrecha de la prohibición de la autoincriminación forzada. En el sentido entendido por el autor,

²¹ POLANSKY, J., *Garantías Constitucionales...*, p. 91.

²² Ello a la luz de lo normado por el art. 29 de la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica) y el principio *pro hómine* como pauta hermenéutica de interpretación. Ver en este sentido PINTO, M., “El principio pro hómine. Criterios de hermenéutica y pautas para la regulación de los derechos humanos” en: “*La aplicación de los tratados de derechos humanos por los tribunales locales*”; Centro de Estudios Legales y Sociales, CELS, Buenos Aires, Argentina, Editorial Del Puerto, 1997, p. 163.

coincido en que una visión anacrónica que limita esta garantía sólo a la manifestación verbal o escrita del acusado, resulta insuficiente y priva a la garantía de su verdadera función tuitiva en la era de las nuevas tecnologías²³.

En esa línea, se advierte que, con el establecimiento de este principio, se podría garantizar que la relación asimétrica entre el imputado y el Estado se vea limitada, evitando que el poder persecutorio estatal sea utilizado de forma arbitraria y que la libertad, la dignidad y la intimidad de la persona actúen como límites infranqueables a la hora del descubrimiento de la verdad. Esto significa que el imputado no cargue con la espada de Damocles sobre su cabeza, puesto que no recae sobre éste el deber de cooperar ni ayudar a la acusación.

Para ir concluyendo con estas cuestiones, vimos cómo el desbloqueo forzado de los dispositivos electrónicos plantea múltiples interrogantes de difícil abordaje, tales como la utilización de la fuerza mínima necesaria sobre la persona imputada, la autorización o injerencia judicial sobre las medidas y/o la asistencia de la defensa en resguardo de los derechos de la persona. Ello, sumado a la falta de previsión legal en los códigos de procedimiento -al menos en el ámbito de la República Argentina-, entiendo que puede resultar un desafío para los próximos años poder establecer un régimen legal que contemple tales circunstancias visto que el Estado -como interesado de llevar adelante una exitosa investigación- bien podría verla frustrada al poder encontrarnos frente a una posible ilicitud de la prueba obtenida. En este sentido, Julio B. J. Maier decía que “se debe, entonces, afirmar finalmente que a la verdad sólo se debe arribar por los medios y en la forma que la ley permite; que, de haberse incorporado al procedimiento un elemento de prueba mediante un acto irregular o mediante un acto regular, cuya posibilidad de realización provenga necesaria y directamente del conocimiento adquirido por un acto irregular, él es invalorable para fundar una decisión judicial, en perjuicio del imputado”²⁴.

La discusión sobre el desbloqueo de dispositivos electrónicos y el contenido declarativo implícito de la biometría nos lleva a una reflexión fundamental: la eficacia policial no puede servir de excusa para el sacrificio de los derechos fundamentales. Tal como señala Jordi Nieva Fenoll, aunque existe una "gran desorientación" policial sobre qué se puede hacer y qué no se puede hacer para ser eficaz sin vulnerar derechos, es imperativo que se encuentre la fórmula para que la investigación sea efectiva "sin renunciar al respeto de dichos derechos bajo ningún concepto"²⁵.

Esta idea se refuerza al afirmar que la búsqueda de la verdad, aunque es un fin del proceso penal, "no puede ser hecha a cualquier costo" y, en definitiva, "la verdad a la que se arribe deberá ser una verdad procesalmente válida", por lo que el fin no justificará los medios y la sociedad debería poder defenderse contra el delito, sin sacrificar los derechos del individuo sometido a proceso²⁶. La "condescendencia jurisprudencial"²⁷ que en ocasiones ha permitido el sacrificio de derechos en aras de la eficacia, es inaceptable y cualquier colisión entre la norma procesal y las garantías constitucionales debe resolverse privilegiando estas últimas, por más grave que fuere el delito.

En este contexto, es crucial subrayar la imperiosa necesidad de un control judicial desde el inicio de la investigación, máxime ante la ausencia de una regulación mencionada para las diligencias policiales que involucran nuevas tecnologías.

Para concluir, entiendo que quien más debería encontrarse interesado en llevar adelante diligencias respetuosas de los derechos fundamentales y legítimas dentro del proceso penal es al Estado persecutor, puesto que "si en el proceso existe un solo cauce de investigación y éste estuvo viciado de ilegalidad, tal circunstancia contamina de nulidad todas las pruebas que se hubieran

²³ ABOSO, G., “Desbloqueo coactivo de datos biométricos y nemo tenetur se ipsum accusare”, Revista Rubinzal Culzoni, Cita: RC D 244/2022, Argentina, 2022.

²⁴ MAIER, J. B. J., *Derecho Procesal Penal*, Tomo I: Fundamentos, Ad Hoc, 2016; p. 663

²⁵ NIEVA FENOLL, J., “La protección de derechos fundamentales en las diligencias policiales de investigación del proceso penal”; Revista de Derecho Procesal Penal, Rubinzal Culzoni, Tomo 2010 1 La defensa penal – I., Revista de Derecho Procesal Penal; Cita: RC D 209/2013; Argentina, 2010.

²⁶ MILL, R., “Prueba Ilícita”, Ed. Rubinzal Culzoni, Revista de Derecho Penal, Tomo: 2001 2 Garantías constitucionales y nulidades procesales – II.; Cita: RC D 2930/2012.; Argentina, 2001.

²⁷ NIEVA FENOLL, J., “La protección de derechos...”, 2010.

originado a partir de aquél"²⁸. En los casos en que el desbloqueo forzado de un dispositivo digital sea considerado un acto ilícito -por violar garantías constitucionales, como la prohibición de autoincriminación-, toda la información obtenida a partir de ese acto podría quedar invalidada como prueba. En consecuencia, permitir que la policía actúe con discrecionalidad y que los jueces convaliden estos procedimientos irregulares, no solo comprometería la legalidad del proceso penal, sino que entiendo que además impone un alto costo institucional: debilita la confianza ciudadana en las instituciones judiciales y erosiona la legitimidad del sistema penal en su conjunto.

5. REPENSANDO UN NUEVO ESTÁNDAR DE PROTECCIÓN. SOBRE LA NECESIDAD DE CONTENER UNA REGULACIÓN ESPECÍFICA

La emergencia evidenciada ante la vida digital de las personas y las implicancias de sus actos con los dispositivos electrónicos que las mismas contienen, exige un nuevo enfoque hermenéutico del principio de no autoincriminación, que abarque no solo las manifestaciones verbales, sino también las rutas tecnológicas de acceso forzado a la subjetividad.

Tal como mencioné anteriormente, entiendo que el límite no tiene que estar dado por la exteriorización o pasividad del acto efectuado por la persona (o el contenido comunicacional del mismo), sino por el resultado jurídico-epistémico: si el Estado obtuviera, por esa vía, información incriminante que el imputado no está obligado a proporcionar de manera directa, ello entonces indefectiblemente configuraría una moderna forma de obtener una autoincriminación forzada.

En ese sentido, ante estos nuevos desafíos que nos impone la globalización y las nuevas técnicas de criminalidad, podemos ver cómo la necesidad de una regulación -además de la garantía contra la autoincriminación como motor central-, impone también un concreto establecimiento en torno a la protección del derecho a la intimidad y a la privacidad (v. arts. 18 y 19 Constitución Nacional; art. 11. 2 Convención Americana de Derechos Humanos; art. 17 del Pacto de Derechos Civiles y Políticos; entre otros).

En este sentido, un teléfono no es únicamente un elemento material, sino también hoy día funciona como una extensión de la vida privada de las personas y, consecuentemente, de necesaria protección en virtud de la sensibilidad de la información que los mismos podrían contener sobre ella. En este aspecto, la injerencia que pudiera tener el Estado, por más "mínima" que pudiese considerarse en el plano "físico", se vuelve mucho más intensa al acceder al contenido digital²⁹. Aquí se ve cómo, por ejemplo, mal puede equipararse esta diligencia con la extracción compulsiva de sangre, o bien un reconocimiento en rueda. En esos casos, la sangre se sabe que es sangre, que el sujeto la tiene y que, cuanto mucho, tan solo se podrá obtener información que de antemano se va a encontrar. Con los dispositivos electrónicos no sucede lo mismo.

Es por tales motivos que se impone la circunstancia de que cualquier acceso a un dispositivo digital deba siempre encontrarse bajo el estricto resguardo de las normas constitucionales y los derechos y garantías establecidos internacionalmente en materia de derechos humanos a fin de no avasallar a cualquier costo, a la persona imputada. Para poder abastecer esta exigencia, entiendo que debe proponerse una cobertura reforzada del *nemo tenetur* en toda forma de compulsión -insisto, sea cual fuera- que derivara en el acceso al contenido de la vida digital de la persona imputada.

El acceso estatal a evidencia digital almacenada en dispositivos personales debe regirse por pautas estrictas derivadas de los principios que estructuran el proceso penal, asentándose, primeramente -y como mencioné- en el principio de legalidad y la reserva de ley, lo que exigirá una regulación expresa, clara y taxativa que determine los supuestos habilitantes, los justificativos y las condiciones bajo las cuales puede ordenarse el desbloqueo forzoso de un dispositivo.

²⁸ MILL, R., "Prueba Ilícita", 2001.

²⁹ ORUÉ, N., "Desbloqueo coactivo del teléfono del imputado mediante obtención de datos biométricos. Algunas consideraciones en torno a su validez constitucional", Estudios sobre jurisprudencia, año 2023, pp. 241-277; con cita a DÍAZ CANTÓN, F. "Prácticas actuales de investigación y recolección de evidencia digital 'versus' garantías de debido proceso", en Ledesma, A. E. (Dir.) – Lopardo, M. (Coord.), *El debido proceso penal*. Volumen 5. Hammurabi, año 2019. Ver digitalizado en <https://repositorio.mpd.gov.ar/jspui/handle/123456789/4752> .

Por otra parte, se advierte que la intervención debe superar un triple test de necesidad, razonabilidad y proporcionalidad. El acceso a este tipo de evidencias debe ser estrictamente necesario -no existiendo una alternativa menos invasiva pero igual de eficaz-, debe ser razonable, dado que tiene que estar justificada en elementos objetivos sospechas fundadas; y debe ser proporcional, en atención a la gravedad del delito, la relevancia de la información que allí se podría obtener y el grado de afectación a éste³⁰.

Para ir concluyendo, otra cuestión trascendental será la voluntariedad del acto. Entiendo que una forma de mitigar la discrecionalidad en la persecución estatal impone la necesidad de incorporar de forma categórica a la normativa, la prohibición de toda forma de coacción, sea física o simbólica, directa o indirecta, destinada a forzar la colaboración del imputado. Solo así podría verse resguardada la posibilidad de incurrir en conductas prohibidas que se traduzcan en una exclusión probatoria del material obtenido y su invalidez como sustento de cualquier acto ulterior.

También, tal como mencionara, se impone el control judicial riguroso, específico y previo como forma de garantizar la validez del acto³¹. En ese aspecto, por vía judicial se podría delimitar el objeto y el alcance temporal de la medida a llevar adelante (evitando las “expediciones de pesca”), así como también establecer mecanismos de control ajenos a la repartición policial encargada -en la provincia de Buenos Aires, casi siempre- de llevar adelante las investigaciones y también contando con la posibilidad de incorporar salvaguardas procesales precisas, tales como la presencia obligatoria del defensor durante la diligencia, el registro audiovisual completo de todo el procedimiento, o bien, un sistema estricto de cadena de custodia que asegure la integridad y autenticidad de la prueba.

Por último, entiendo que también puede ser útil fundar su validez cuando el contenido buscado esté previamente individualizado -haciendo las veces de un test de *foregone conclusion* a la inversa-.

Solo en estos casos entiendo que, bajo estos estándares, se superará la fórmula clásica establecida para garantizar la autoincriminación forzada y podría el Estado, con los parámetros antes establecidos, asegurar que las garantías no fueran un obstáculo formal, sino más bien, un límite material a poder franquear frente a ciertos entornos digitales.

6. CONCLUSIÓN

A lo largo de este trabajo se han intentado examinar las principales problemáticas que plantea el desbloqueo compulsivo de teléfonos celulares en el marco del proceso penal y la evidente tensión que presenta frente a la garantía contra la autoincriminación y la intimidad de toda persona sometida a proceso penal. Pues bien, primeramente, se advirtió que el avance vertiginoso de la tecnología no sólo ha transformado a los medios de investigación frente a las nuevas formas de criminalidad que el mundo actual se encuentra experimentando, sino que ha puesto en evidencia las falencias normativas y los límites imprecisos que el marco jurídico tradicional presenta para dar respuesta a estos nuevos desafíos.

En este contexto, ha quedado claro que la obtención de evidencia digital no puede regirse únicamente por criterios de eficacia investigativa, sino que la validez de estas medidas debe evaluarse a la luz de los principios rectores de todo Estado de Derecho: el respeto por la dignidad de la persona, la prohibición de declarar contra uno mismo y la necesidad de preservar un ámbito inviolable de privacidad, entre algunas de las garantías fundamentales que reposan sobre todo ciudadano. Obligar a un imputado a desbloquear su dispositivo sin las debidas garantías -y sea el método que fuere-, implica una forma de autoincriminación que debilita las bases mismas del diseño procesal penal y constitucional actual.

Asimismo, se advierte la urgencia de que los poderes legislativos asuman un rol protagónico en la regulación de esta materia, toda vez que sin normas que establezcan límites claros, controles efectivos y garantías procesales robustas, continuará persistiendo una incertidumbre jurídica y el

³⁰ BUGLIONE, M., “El desbloqueo forzoso ...”, 2024.

³¹ NIEVA FENOLL, J., “La protección de derechos...”, 2010.

riesgo de sufrir arbitrariedades sobre las personas sospechadas en el marco de una investigación criminal, lo cual tan solo logra desdibujar las bases constitucionales antes mencionadas frente al poder punitivo de los Estados.

En ese sentido, entendiéndolo a la evidencia digital como parte central de la agenda penal contemporánea, se permite colegir que resultará indispensable repensar conceptos tradicionales a la luz de esta nueva realidad que se avecina y la promoción de instancias de capacitación específicas para operadores jurídicos y fuerzas de seguridad o investigación delictiva involucradas.

En definitiva, frente a las lagunas normativas y los abordajes jurisprudenciales dispares en torno a cómo proceder frente al reto que propone la evidencia digital, entiendo que el desafío consistirá en armonizar los fines legítimos de la persecución penal con los principios constitucionales que rigen el proceso penal, el cual sólo podrá garantizarse mediante la fijación de un nuevo estándar normativo -claro, garantista y adaptado al contexto actual- para evitar así que el uso de estas herramientas de investigación termine debilitando, por la vía de hecho, los límites del poder punitivo y la legitimidad del sistema judicial.

BIBLIOGRAFÍA

- ABOSO, G. en “Desbloqueo coactivo de datos biométricos y nemo tenetur se ipsum accusare”, Revista Rubinzal Culzoni, Cita: RC D 244/2022, 2022;
- BINDER, A., *Introducción al derecho procesal penal*, 2da. Ed. actualizada y ampliada. Ad Hoc, Ciudad Autónoma de Buenos Aires, 2016;
- BLANCO, H., “Prohibición de autoincriminación, Derecho a la intimidad y apertura compulsiva de smartphones por métodos biométricos”, en DUPUY, D. et al. (dirs.): *Tratado internacional sobre procedimiento criminal, transnacional y digital*, Tirant lo Blanch, Valencia, 2025;
- BRUZZONE, G., “La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal”, AA.VV. *Estudios sobre Justicia Penal, Homenaje al Profesor Julio B. J. Maier*. Editores del Puerto, Buenos Aires, 2005;
- BUGLIONE, M. J.; “El desbloqueo forzoso de celulares. Validez constitucional y estado actual de la jurisprudencia”, Temas de Derecho Penal. Errepar, Argentina, 2024;
- CARRIÓ, A. D., *Garantías Constitucionales en el proceso penal*, 6ta. Ed., 6ta. Reimp.. Hammurabi, Argentina, 2023;
- DÍAZ CANTÓN, F., “Prácticas actuales de investigación y recolección de evidencia digital 'versus' garantías de debido proceso”, en LEDESMA, A. E. (Dir.) – Lopardo, M. (Coord.), *El debido proceso penal*. Volumen 5. Hammurabi, Argentina, 2019;
- FAVAROTTO, R. S.; “El derecho a oponerse a colaborar con la acusación”; Publicado en: DPyC 2025 (febrero), 93; Cita: TR LALEY AR/DOC/65/2025; Argentina, 2025;
- MAIER, J. B. J., *Derecho Procesal Penal, Tomo I: Fundamentos*, Ad Hoc, Buenos Aires, 2016;
- MILL, R., “Prueba Ilícita”, Revista de Derecho Penal, Rubinzal Culzoni, Tomo: 2001 2 Garantías constitucionales y nulidades procesales – II.; Cita: RC D 2930/2012; Argentina, 2001;
- MILLER, C. H., “¿Pueden las fuerzas de seguridad forzar el desbloqueo de un dispositivo con datos biométricos del sospechoso? Acerca de los recientes fallos de la justicia de los Estados Unidos”. Publicado en: LA LEY 03/07/2019, 6 • LA LEY 2019-C, 536;
- NIEVA FENOLL, J., “La protección de derechos fundamentales en las diligencias policiales de investigación del proceso penal”; Revista de Derecho Procesal Penal, Rubinzal Culzoni, Tomo 2010 1 La defensa penal – I., Revista de Derecho Procesal Penal; Cita: RC D 209/2013; Argentina, 2013;

- ORUÉ, N., “Desbloqueo coactivo del teléfono del imputado mediante obtención de datos biométricos. Algunas consideraciones en torno a su validez constitucional”, Estudios sobre jurisprudencia; MPD; Buenos Aires, 2023;
- PÉREZ BARBERÁ, G., “Nuevas tecnologías y libertad probatoria en el proceso penal”, en Nueva Doctrina Penal, 2009/A;
- PINTO, M.: “El principio pro homine. Criterios de hermenéutica y pautas para la regulación de los derechos humanos”; en: “La aplicación de los tratados de derechos humanos por los tribunales locales”; pág. 163; Centro de Estudios Legales y Sociales, CELS, Ed. Del Puerto, Buenos Aires, Argentina, 1997;
- POLANSKY, J., *Garantías Constitucionales del Procedimiento Penal en el entorno digital*; Hammurabi, Buenos Aires, año 2020;
- SALT, M., “Allanamiento remoto ¿Un cambio de paradigma en el registro y secuestro de datos informáticos?”, en *Cibercrimen II*, 1a edición; Edit. BdeF, Montevideo-Buenos Aires, 2018.

Jurisprudencia de EEUU:

- SCOTUS, 384 U.S. 436 (1966);
- SCOTUS, 348 U.S. 757 (1966);
- SCOTUS, 425 U.S. 391 (1976);
- SCOTUS, 465 U.S. 605 (1984);
- SCOTUS, 487 U.S. 201 (1988);
- SCOTUS, 530, U.S., 27 (2000);
- SCOTUS 573 U.S. 373 (2014);
- Commonwealth of Virginia, Second Judicial Circuit, *Commonwealth of Virginia v. Baust*, Case Nro. CR-14-1439, (28/102014).;
- United States District Court, Northern District of California; “*Order denying application for a search warrant; order sealing application*”; Case N° 4-19-70053, (2019);
- USDC, District of Idaho, Caso 1:19-mj-10441 *REB*, (2019);
- Indiana Supreme Court; Supreme Court Case No. 18S-CR-595; *Katelin Eunjoo Seo - Appellant (Defendant) v. State of Indiana -Appellee (Plaintiff)-*, (2020).

Jurisprudencia Argentina:

- CSJN, “Mendoza” (1864);
- CSJN, “Diario El Atlántico” (1971);
- CSJN, “Cincotta” (1963);
- CSJN, “H. G. S.” (1995);
- CSJN, “Zambrana Daza” (1997);
- CSJN, “Rau” (2016);
- Cámara Federal de Bahía Blanca, Expediente nro. FBB 3139/2022/1/CA1, caratulado: “Incidente de Reposición: ‘MORA, Brisa Aylén por infracción ley 23.737 (art. 5 inc. c)’”; 27/05/2022.

Jurisprudencia interamericana:

- Corte Interamericana de Derechos Humanos, *Caso Escher y Otros vs. Brasil*; Sentencia de 6 de julio de 2009 (Excepciones Preliminares, Fondo, Reparaciones y Costas).