PRÓLOGO

Es para mí un placer enorme prologar la obra de Jonathan Polansky, a quien conozco de la Facultad de Derecho de la Universidad de Buenos Aires, ámbito académico en el que se graduó y en el que continúa trabajando como docente e investigador.

Su libro se inscribe en una corriente moderna de autores que afronta el difícil desafío de analizar las implicancias que las nuevas tecnologías informáticas generan en el derecho penal, procesal penal y en la práctica de los tribunales. La construcción de una doctrina especializada y la consolidación de prácticas jurisprudenciales sobre esta temática resultan fundamentales para el mejoramiento del sistema penal de nuestro país y la región. El desafío que plantean las TIC al sistema penal en su conjunto requiere de ideas jurídicas innovadoras, nuevos principios, adaptación de garantías existentes, etcétera, frente a una realidad marcada por el cambio vertiginoso que produce la tecnología en todos los ámbitos de la sociedad. Es evidente que la tecnología avanza más rápido que el derecho y, por tal motivo, origina importantes distorsiones en el funcionamiento de la justicia que se traduce tanto en "pérdida de eficiencia" como en prácticas de investigación aceptadas acríticamente en las investigaciones penales y que implican un menoscabo de garantías fundamentales, especialmente la intimidad y el derecho de defensa.

El libro de Jonathan aborda precisamente el tema de las garantías constitucionales del proceso penal en entornos digitales. Para ello se vale de un bagaje importante de información teórica, un interesante análisis de derecho comparado (especialmente de la jurisprudencia de EE. UU.) y un enfoque "práctico" que le permite buscar soluciones a problemas concretos que ya se presentan en nuestras investigaciones penales, aunque, en la mayoría de los casos, ni siquiera son advertidos ni han generado debates jurisprudenciales o resoluciones de tribunales superiores[1].

[1] Muchos de los problemas de los nuevos medios de prueba e investigación en entornos digitales pueden generar afectaciones a garantías tradicionales del proceso penal que no están sien-

Al estudio teórico del tema y el análisis de jurisprudencia, Polansky le suma la experiencia adquirida en su trabajo en el Ministerio Público Fiscal, lo que le permite proponer soluciones a cuestiones concretas. Este enfoque le otorga mayor interés a la obra: aporta ideas y arriesga propuestas de solución para supuestos fácticos determinados que hoy ponen en "conflicto" las garantías constitucionales del proceso penal entendidas todavía en un sentido tradicional, más ligado al mundo físico que a la nueva realidad que genera la virtualidad y la digitalización.

El tema no podía tener más actualidad e importancia práctica. Hace ya tiempo que venimos advirtiendo que la prueba digital va a generar un "cambio de paradigma" en el proceso penal. Es más, ya es posible advertir una tendencia paulatina de reemplazo de la prueba física por la prueba digital en la investigación de todos los delitos. No se trata solamente de un tema vinculado de manera exclusiva a la investigación de los delitos informáticos, sino, antes bien, los elementos de prueba digital aparecen como fundamentales en la investigación de cualquier delito, sea este tecnológico o no. En lo personal, ya no me quedan dudas de que en un futuro, cada vez más cercano, la prueba digital tenderá a relegar a un segundo plano a la prueba física, que servirá como complemento de elementos de prueba obtenidos en formato digital[2]. Este proceso de reemplazo de la prueba física por la prueba digital se ha profundizado y acelerado como consecuencia de la pandemia Covid-19 que afecta a todos los países.

Paradójicamente, estamos inmersos en este "cambio de paradigma" del proceso penal acelerado, sin haber realizado modificaciones normativas importantes y atados a viejas prácticas. Esto es, hemos ingresado a una nueva etapa histórica del proceso penal, pero sin modificar los códigos procesales penales. Es evidente la necesidad de regular de manera urgente los medios de prueba en entornos digitales[3], dejando de lado la práctica asumida por nuestros tribunales de utilizar analógicamente los medios de prueba pensados para la prueba física. Esta práctica "cortoplacista" aceptada por nuestra jurisprudencia (quizá por necesidad frente al retraso del legislador), genera problemas tanto para la eficiencia de las investigaciones

---

do analizadas por nuestra jurisprudencia ni planteadas adecuadamente por las defensas técnicas. Creo que a esta altura resulta evidente la trascendencia de la capacitación de los operadores del sistema y la incorporación de materias específicas en el currículo de las facultades de derecho.

[2] A modo de ejemplo, para acreditar si una persona estuvo en un determinado lugar en un momento determinado los datos de geolocalización de sus dispositivos o los archivos digitales de cámaras son más útiles que la declaración de testigos. Es fácil imaginar que estos medios de prueba más sencillos de obtener y más fiables reemplazarán a la prueba testimonial en estos supuestos.

[3] Por otra parte, la incorporación a la legislación procesal penal de un set de medios de prueba básicos para la incorporación al proceso de prueba digital constituye una obligación asumida por el Estado argentino a partir de la adhesión a la Convención de Budapest.

como para una adecuada protección de las garantías constitucionales. El Capítulo IV del libro, dedicado al "análisis de información contenida en dispositivos informáticos", constituye un ejemplo paradigmatico de los problemas que genera esta práctica perniciosa de aplicar normas procesales por analogía a situaciones claramente no asimilables. Pensar que el registro y secuestro de datos de un dispositivo informático puede quedar alcanzado o correctamente regulado por las normas previstas para el allanamiento y secuestro en espacios físicos aplicadas por analogía es un despropósito difícil de comprender. El capítulo mencionado aporta aún más elementos. El autor recorre a través del análisis de la doctrina y la jurisprudencia de EE. UU. situaciones que podemos asimilar a nuestro medio. De esta manera nos plantea diferentes escenarios útiles, tanto para analizar posibles soluciones con la legislación procesal vigente en nuestro país a casos que ya suceden en la práctica de nuestros tribunales, como para considerar posibles reformas legislativas. Las diferencias entre el allanamiento en el mundo físico y digital, las dificultades de aplicación de la doctrina de la *plain view* en entornos digitales, la diferencia entre "registro" y "peritaje" en el entorno digital, etcétera, son todos temas abordados con ejemplos jurisprudenciales y referenciados a casos prácticos que guían la obra.

El Capítulo I está dedicado a uno de los temas que más debates jurídicos y prácticos está planteando al derecho procesal penal y a la cooperación internacional en materia penal[4]: la "naturaleza" que debe asignarse y la protección constitucional que merecen los *metadatos*. La necesidad de proteger la intimidad frente al aumento de poder de investigación de los Estados mediante nuevas herramientas tecnológicas, ha reabierto el debate sobre la clásica distinción de "datos de abonado", "tráfico" y "contenido", y, conforme a ella, cuál es el grado de protección a la intimidad que merecen. Las modernas posibilidades de tratamiento masivo de datos y la utilización de programas especiales (algunos con técnicas de IA) que permiten construir perfiles personales a través de datos de tráficos, geolocalización y metadatos en general, ha motivado cambios jurisprudenciales en el derecho comparado. Fundamentalmente se han abierto nuevas controversias sobre la necesidad de autorizaciones judiciales especiales para la obtención de determinados datos que antes tenían estándares menores de protección.

El libro analiza muchos de estos supuestos, tanto en la jurisprudencia de la Corte de EE. UU. como de la Corte de Justicia de la Unión Europea, y hace el intento de transpolar algunas de sus conclusiones a la situación en nuestro medio jurídico comparando con los escasos antecedentes jurisprudenciales existentes. Así arriba a la conclusión de la necesidad de proteger estos datos cuando su recolección implique afectar seriamente la intimidad. Abre de esta manera un criterio diferenciador en-

[4] Tanto la cooperación entre países como la regulación de la cooperación de empresas del sector privado respecto a solicitudes provenientes de extraña jurisdicción (cooperación asimétrica).

tre los "metadatos que afectan la intimidad" y aquellos que no, que requerirá de nuevos trabajos que profundicen la idea.

El Capítulo II está dedicado a uno de los problemas modernos surgido de la necesidad de los Estados de hacer frente a las dificultades que las tecnologías de encriptación plantean a las investigaciones penales. Estas dificultades, en términos de eficiencia, han justificado la necesidad de nuevos medios de investigación más intrusivos de la intimidad como es el uso de agentes encubiertos digitales o la utilización por parte del Estado de programas maliciosos para obtener datos de manera subrepticia de los dispositivos de un imputado (técnicas de *remote forensic*) o la dirección IP real de quien utiliza técnicas de anonimato. El autor se dedica en este capítulo a un tema puntual de esta nueva problemática (denominada por algunos autores como "cripto controversia"): el desbloqueo de teléfonos celulares mediante el uso "compulsivo" de datos biométricos del imputado. Su análisis, basado en los desarrollos de la jurisprudencia de EE. UU., resulta de sumo interés teniendo en cuenta que la situación fáctica ya se ha planteado en nuestros tribunales y no hay una jurisprudencia uniforme ni, mucho menos, una regulación procesal especial que aborde estos supuestos.

El libro introduce, en el Capítulo V, otro tema novedoso en nuestro medio jurídico: el análisis de la situación jurídica de las "copias forenses" y la necesidad de regular tanto su utilización durante el proceso como el destino de la enorme cantidad de datos personales que contienen[5], no solamente vinculados al objeto procesal que justificó su obtención sino también de los datos que nada tienen que ver con la investigación del delito que puede haber justificado la medida de secuestro[6]. El autor propone diferentes situaciones fácticas y reflexiona sobre la protección constitucional de las copias forenses y las implicancias prácticas que tiene para el proceso penal. Las conclusiones de este capítulo son también un interesante insumo para considerar al momento de pergeñar la reforma procesal que introduzca las normas necesarias para prever de manera especial la prueba digital.

Las ventajas que tiene realizar el análisis de información digital sobre copias forenses han determinado que, de a poco, se constituya en la regla (y no la excepción) cuando los agentes estatales que están a cargo de la medida cuentan con los recursos y posibilidades técnicas. La realización de copias forenses es hoy una "buena

[5] El tema del destino de las copias forenses una vez finalizado un juicio no ha merecido aún, hasta lo que conozco, tratamiento en nuestra jurisprudencia.

[6] A modo de ejemplo, la copia forense puede contener correos electrónicos, fotos familiares, datos de navegación, etcétera, que no se vinculen con el objeto procesal y que no son ni siquiera analizados o utilizados en la investigación pero que quedarán en poder del Estado. También pueden contener elementos de prueba de otro delito no alcanzado por el objeto procesal que motivó el secuestro.

práctica" aceptada por los especialistas y así está documentado en las principales guías y protocolos especializados. Reemplazar el secuestro de los dispositivos físicos por la realización de copias forenses aseguradas con códigos *hash* su integridad, permite en muchos supuestos limitar los efectos que la medida puede generar al titular de los soportes de información secuestrados y a terceros que se pueden ver afectados por la medida. Pensemos, a modo de ejemplo, un banco, una empresa, un estudio jurídico, etcétera, al que le secuestraran todas las computadoras o los servidores. El secuestro de los dispositivos implicaría que no puedan continuar trabajando normalmente por un largo período de tiempo. Asimismo, trabajar sobre la copia forense en lugar del dispositivo original permite dar más seguridad a las medidas que se realizan, ya que siempre serán "reproducibles" en términos procesales. Incluso cuando se secuestran los dispositivos físicos de almacenamiento, realizar los trabajos de búsqueda de datos útiles para la investigación o los análisis periciales sobre copias forenses y no sobre los "originales" presenta múltiples ventajas que han determinado a los especialistas a optar por este sistema de trabajo.

El autor se pregunta: ¿Qué debería hacer el Estado con esos archivos de datos (copias forenses) con posterioridad a su utilización en el proceso? ¿Puede el Estado conservarlos y utilizar sus datos en otras investigaciones? ¿Pueden reproducirse esas copias? ¿Es legítimo que el Estado decida entregar copias forenses que pueden contener gran cantidad de datos que nada tienen que ver con el objeto procesal investigado a terceras partes como un querellante o un coimputado para que realicen sus tareas de búsqueda o pericia por separado? En lo personal, vengo advirtiendo hace tiempo los problemas que puede significar en los procesos acusatorios la entrega a los diferentes sujetos procesales de copias forenses para que realicen sus trabajos de análisis de manera separada conforme a su "teoría del caso". Pero no había reflexionado sobre los otros problemas que plantea el autor.

Jonathan Polansky nos ilustra sobre las soluciones dadas a muchos de estos cuestionamientos en la jurisprudencia de EE. UU. y arriesga posturas sobre cómo debería solucionarse en nuestro sistema. Sin duda, constituye un insumo importante para debatir un tema ya presente en nuestra práctica tribunalicia pero aún no solucionado.

El Capítulo III plantea una de las problemáticas más modernas y desafiantes para el proceso penal: la utilización de algoritmos, programas e inteligencia artificial en técnicas forenses de obtención de datos. Estas herramientas funcionan conforme a códigos fuente o algoritmos que, generalmente, no podrán ser conocidos por la defensa (tampoco por los jueces y fiscales). Jonathan nos plantea el uso de herramientas que arrojan importantes elementos de prueba pero que trabajan de manera "automática" conforme a códigos de programación que no siempre (generalmente no) pueden ser revisables por la defensa. Estos programas son cada vez más utilizados en el proceso penal. El autor no solo realiza una importante descripción de muchos de ellos, que ya se usan diariamente en nuestro medio (por ejemplo, el

UFED que permite extraer datos de teléfonos celulares), sino que agrega los interesantes desarrollos de la jurisprudencia de EE. UU. sobre los posibles problemas que pueden significar para las garantías del imputado. El análisis resulta apasionante. Se trata de herramientas forenses cuya utilización crece diariamente en los procesos penales favoreciendo la eficiencia de las investigaciones, pero que requerirán de análisis que permitan establecer en el proceso penal la forma de asegurar la confiabilidad de los datos obtenidos y que estas no impliquen, por los mecanismos que utilizan para la obtención de los datos, una violación a las garantías.

Polansky arriesga algunas propuestas concretas pensando en nuestro medio, que seguramente serán el inicio de estudios más profundos que espero, fervientemente, encare.

Mis felicitaciones a Jonathan por su obra y una invitación especial a los lectores a reflexionar sobre los temas planteados. La necesidad de encontrar un balance adecuado entre la eficiencia del sistema de persecución penal y las garantías constitucionales del proceso penal en entornos digitales es uno de los desafíos más importantes al que se enfrenta el sistema penal moderno. Como señalé antes, el libro es un insumo importante en esta tarea, tanto para los debates jurisprudenciales como para definir una futura regulación procesal. El autor plantea propuestas que deseo sean un disparador de estudios y futuros trabajos.

MARCOS SALT[7]

Buenos Aires, agosto del 2020

[7] Doctor en Derecho (Universidad Nacional de Córdoba). Profesor de Derecho Penal y Procesal Penal (UBA). Director del Posgrado de Cibercrimen y Evidencia Digital de la Facultad de Derecho (UBA).